BUSINESS IN THE CROSSROADS OF DIGITAL TRANSFORMATION: ARE THERE LEGAL CONSEQUENCES TO THE SAME?

Dhritiman Sarma
BA LLB Semester 1st, National University of Advanced Legal Studies, Kochi , Kerala, India
Email: dhritimansarma2017@nuals.ac.in

Abstract
Modern business landscape's defining trend is digital transformation, which is transforming how businesses run, communicate with customers, and engage in global competition. This transition has been especially significant in India, a nation with a rapidly expanding digital economy. While the digital transformation presents enormous prospects for innovation, efficiency, and growth, it also presents organizations with a challenging and intricate web of legal repercussions. In this paper, the digital revolution of Indian enterprises is examined, as well as the legal ramifications that come along with it. India has seen a significant digital change recently, fueled by a number of causes, consisting of: Digital Infrastructure: The Digital India project of the Indian government has been instrumental in the growth of the internet on mobile devices, electronic payment methods, and rural connection. Consumer Behavior: Indian customers' expectations and purchasing behaviors have altered dramatically as a result of the adoption of digital technology, such as smartphones and e-commerce platforms. Business processes: Businesses in all sectors have embraced digital technology in an effort to improve customer experiences, streamline operations, and use data analytics to make better decisions. Start-up Ecosystem: The number of technological start-ups in India has increased, stimulating innovation and accelerating the digital transformation of industries including fintech, health tech, and agritech.

Key words:
Digital transformation, Business, Consumer, Cyber Law, Consumer Protection.

1. INTRODUCTION

Digital transformation has become a crucial strategy for businesses wanting to stay competitive and relevant in today's quickly changing corporate environment. The phrase "digital transformation" refers to a broad range of technical developments, process enhancements, and cultural transformations that radically alter how firms' function, interact with their clients, and provide value. For survival and success in the digital era, this transition is not just a choice, but rather a requirement. A corporation's operations, procedures, goods, services, and contacts with customers are all included in the term "digital transformation," which describes the thorough integration of digital technology into all aspects of an organization. It includes a number of important elements, some of which are covered in the paragraph below.

Businesses are adopting the most recent digital tools and technology, such as automation, cloud computing, artificial intelligence (AI), the Internet of Things (IoT), and data analytics along with using data to gain understanding, make wise decisions, and forecast trends. Data is frequently referred to as the digital economy's new currency. Putting the consumer at the centre of all corporate endeavors and utilizing digital platforms to provide seamless, personalized interactions, promoting an innovative, flexible, and digitally literate culture across the entire organization. The following are some of the major issues that are driving the necessity of digital transformation in businesses:

Today's consumers demand individualized, quick, and technologically enabled experiences. To be competitive, businesses must adjust to fulfil these expectations. Rapid technological advancements present both benefits and dangers. Organizations can innovate when they embrace technology, but if they don't, more tech-savvy competitors may disrupt them. Businesses can now expand internationally more easily thanks to digital tools and the internet, but doing so exposes them to international competition. Businesses that undergo digital transformation can grow and successfully compete on a global basis. There is an extraordinary amount of data produced in the digital age. Businesses that use this data well can learn important things about consumer behavior, market trends, and operational efficiency.

Technology can reduce operational costs through automation, remote work capabilities, and resource allocation optimization, personalized interactions and efficient service delivery lead to higher customer satisfaction and loyalty also Digital transformation fosters a culture of innovation, encouraging new ideas. These are just a few of the obvious benefits that have been brought about by the shift to digital. In the current study, an effort is made to examine both the corporate sector's digital revolution and its legal ramifications.

2. REVIEW OF THE LITERATURE

The digital revolution is radically and permanently altering the corporate landscapes around the world. This revolution alters how firms operate, interact with consumers, and generate value. One aspect of this transformation is the integration of digital technology into various business operations. Organisations embarking on a digital transformation, however, must navigate a complex web of legal ramifications. The key legal concerns surrounding enterprise digital transformation are examined in this review of the literature, including data privacy, intellectual property, contracts, cybersecurity, compliance, and more.

Security and data privacy are two of the major concerns relating to the digital shift. The explosion of data collection, processing, and storage raises a number of legal difficulties; some of the legal frameworks that have an effect on businesses everywhere are covered in the paragraphs that follow.

Strict regulations are imposed for the collection and processing of personal data by the General Data Protection Regulation (GDPR). It is a European regulation that affects the entire world. Due to deterrent fines and mandated data breach notifications, businesses must prioritise data protection (Bélanger & Crossler, 2019). The California Consumer Privacy Act (CCPA), also known as "GDPR-lite," applies to California citizens and requires businesses to publish their data practises, provide means to opt out, and grant requests for data access (Wieringa.J et. al. 2021). Laws requiring businesses to notify affected parties and authorities of data breaches have been passed in a number of nations. Failure to comply may have legal ramifications. However, companies run the risk of facing legal ramifications if they don't adopt robust data security protocols. Data breaches have serious repercussions, such as fines, damage to one's reputation, and compensation for individuals affected .

The legislation pertaining to intellectual property (IP) is another crucial one for businesses.Intellectual property considerations are essential when employing new digital tools and technology in business, as will be covered in the paragraphs that follow.

Programme Licencing: Appropriate software and technology licencing agreements are essential to preventing intellectual property infringement. The rise of open-source software has increased the difficulty of licencing. Copyrights and patents A common phase in the development of digital solutions is the creation of intellectual property, such as patents, copyrights, and trademarks. It's important to protect and uphold these intellectual property rights (Khan et al., 2020). Making legal arrangements while working together in business is another crucial factor to consider. The process of digital transformation typically entails collaboration with partners and outside companies like:

• Cloud Services and Outsourcing: Ji et al. (2017) assert that contractual agreements with cloud service providers and outsourcing partners must precisely specify roles, service requirements, and dispute resolution procedures.

• Service Level Agreements (SLAs): SLAs, according to Beirne and Cahalane (2019), outline performance standards, uptime guarantees, and penalties for noncompliance in digital services.

Another area where law and business conflict is with internet-based business and transactions. E-commerce and digital transactions have legal implications for the enforcement of contracts and consumer protection: Online Agreements: Online contracts, such as user agreements and terms of service, must be made sure to be legal and enforceable (Hossain et al., 2018). rules for consumer protection: E-commerce businesses are required to abide by consumer protection laws that cover open pricing, ethical business practises, and customer rights (Cavusoglu et al., 2015). Cybersecurity and responsibility are important legal considerations for business enterprises. The increased danger of cyberattacks and data breaches poses significant legal risks: Cybersecurity Liability: Organisations may be held liable for failing to adequately protect customer data. The development of cybersecurity policies, incident response plans, and cyber insurance are examples of risk mitigation strategies (Verheyden et al., 2013). Third-Party Liability: The process of digital transformation typically involves third-party vendors and partners. To identify who would be liable for security breaches or other issues, contract liability clauses should be carefully reviewed and crafted.

As technology develops, regulatory frameworks are particularly susceptible to change in the following areas: Industry-Specific Legislation: Some industries, like the financial industry (Dodd-Frank Act) and the healthcare sector (HIPAA), have specific legislation governing digital practises. Compliance is important, say Raghupathi et al. (2019). Due to the changing nature of digital technology, organisations must regularly monitor legal revisions and adjust their practises .Businesses need to have procedures in place to ensure the legal validity and preservation of electronic data and documents, according to Davenport et al. (2017). Employees need to be trained on the best practices for digital security, and the organisation should have clear policies and procedures in place for the use of digital tools and technology . Thus, the literature review gives a glimpse of the current legal discourse on business digitization and its myriad legal implications.

3. LEGAL REPERCUSSIONS OF BUSINESS DIGITAL TRANSFORMATION

The General Data Protection Regulation (GDPR) and data privacy laws in India are only two of the many international policies that apply to data privacy and security, which are essential components of the digital transformation. We shall examine the GDPR and Indian data privacy laws here: The European Union (EU) introduced GDPR, a thorough data protection policy, in May 2018. Although it primarily affects EU member states, it has a global influence and has an effect on companies all over the world that handle the personal data of EU citizens.

1. Consent: Under GDPR, organisations are required to get individuals' explicit and unequivocal consent before collecting and using their personal data. This consent ought to be simple to revoke.

2. Data Protection Officers (DPOs): To ensure compliance, organisations that process significant amounts of personal data or carry out specific sorts of processing activities must employ a DPO.

3. Data Subject Rights: The GDPR gives people a number of rights, including the opportunity to access their data, have their data erased, and have their data portable.

4. Data Breach Notification: Within 72 hours of becoming aware of a data breach, organisations are expected to notify the relevant data protection authorities as well as any impacted people.

5. Data Protection Impact Assessments (DPIAs): To evaluate and reduce privacy concerns, DPIAs are necessary for high-risk data processing operations.

6. Cross-Border Data Transfers: Under GDPR, organisations must apply suitable safeguards like Standard Contractual Clauses (SCCs) or Binding Corporate Rules (BCRs) in order to transfer personal data outside the EU to nations with insufficient data protection laws.

3.1. Indian regulations governing data privacy:

The Personal Data Protection Bill (PDPB), which was tabled in Parliament in 2019, is the most prominent law and regulation in India that governs data privacy and protection.

Important features of the Personal Data Protection Bill (PDPB)

1. The PDPB suggests localising personal data, which means that some types of personal data should only be processed and stored in India. Multinational corporations' activities may be impacted by this.

2. Similar to GDPR, the measure places a strong emphasis on obtaining informed consent before processing personal data and outlines the legal grounds for doing so.

3. Data Subject Rights: The law provides data subjects with the same access, rectification, and erasure rights as the GDPR.

4.Data Protection Authority: The bill calls for the creation of the Data Protection Authority of India (DPA) to monitor adherence to the rules and enforce them.

5. Data Breach Notification: Similar to GDPR's data breach notification rules, organisations are required to notify the DPA and impacted persons of data breaches.

6. Cross-Border Data Transfers: The law tackles cross-border data transfers and lays out regulations for them, including possible localization rules for the data.

It's crucial to remember that the PDPB is still under consideration by lawmakers and has not yet become a law. But it shows that India is committed to tightening privacy and data protection laws to meet international norms.

3.2. Indian Intellectual Property Laws

For the protection of intellectual property, such as patents, copyrights, trademarks, and trade secrets, India has a strong legal system. The laws and rules that apply include:

1. The Indian Patent Act, 1970 is the statute that controls the issuance and defence of patents in India, including those for software. Software as a whole is not patentable, however inventions relating to software may qualify for patent protection.

2. The Copyright Act of 1957: This law protects literary, theatrical, musical, and creative works—including computer software—from infringement. Upon the production of the work, the creator is immediately given copyright.

3. The Trademarks Act, 1999: This law governs the filing of trademark applications and their protection in India, especially those pertaining to software and technological goods.

4. The Information Technology Act of 2000: This law aids in establishing the legitimacy of electronic contracts, such as software licences, by containing requirements relating to electronic records and digital signatures.

3.3. Technology and Software Licencing in India:

Software and technology licencing refers to the transfer of ownership (licensor) rights to another party (licensee) on certain terms and conditions, including the right to use, modify, or distribute the software or technology. Software and technology licencing agreements in India are governed by a number of legal factors, including:

1. Software or technology licence agreements specify the terms and conditions of use, including the license's scope, limitations, costs, and length.

2. Intellectual Property Rights: Whether it is a copyright licence, patent licence, or a combination of both, the agreement must describe the intellectual property rights being licenced.

3. Usage limits: The licence agreement could have usage limits, like caps on the number of users, regional restrictions, and no-reverse-engineering clauses.

4. Payment Terms: The payment terms, including licencing fees, royalties, and any maintenance or support fees, should be spelt out in the agreement.

5. Warranty and liabilities: It is important to specify any guarantees and liabilities for damages. Certain guarantees may be disclaimed by the licensor, and responsibility may be restricted to a certain degree.

6. Renewal and Termination: The terms of the agreement should outline how the licence may be terminated and renewed.

7. Dispute Resolution: The agreement should include specifics about how disputes will be resolved, such as through arbitration or litigation.

8. Compliance with Export Control rules: The agreement should address compliance with export control rules if the software or technology is covered by such laws.

9. Protection of Trade Secrets: If the technology involves the use of trade secrets, the contract should contain clauses that safeguard these sensitive details.

10. Governing Law: The agreement should specify the governing law and the relevant jurisdiction.

To make sure that their interests are safeguarded, licensees and licensors of software and technology must both carefully analyse and negotiate licencing agreements. Furthermore, these contracts' terms must adhere to Indian IP laws and rules. Depending on the terms of the agreement, parties may seek legal remedies through litigation or alternative dispute procedures, including arbitration or mediation, in the event of a dispute or breach of a software or technology licencing agreement. In conclusion, special IP rules and regulations apply to the licencing of software and technology in India. Understanding and abiding by these regulations is essential for both technology makers and users to ensure the legal use and preservation of intellectual property rights as the digital transformation of company operations proceeds. Due to the growing use of e-commerce and online transactions in India, consumer protection regulations are essential in ensuring that customers' rights and interests are protected. India has particular laws in place to safeguard

customers making online purchases. We will examine the main facets of India's consumer protection regulations with regard to online and e-commerce transactions below:

3.4. Indian Consumer Protection Laws

3.4.1.2019 Consumer Protection Act:

The outdated Consumer Protection Act of 1986 was replaced by a comprehensive Consumer Protection Act that was enacted in India in 2019. The new law seeks to strengthen consumer rights and offer a strong framework for protection of consumers, notably in the context of online shopping.

Key Requirements:

- Definition of Consumer: The definition of "consumer" in the act is broad and includes people who make online purchases of products and services.
- Responsibilities of E-commerce Platforms: According to the legislation, e-commerce platforms are "service providers" and are accountable for carrying out duties like verifying the legitimacy of vendors and revealing pertinent information about their customers.
- Consumer Rights: The act outlines a number of consumer rights, such as the right to information, the ability to exchange items or discontinue services, and the right to be shielded from deceptive marketing and unfair business practises.
- Consumer Disputes: The act creates commissions for the prompt adjudication of consumer complaints, particularly those involving online transactions, at the district, state, and national levels.
- Product Seller Liability: For subpar goods or subpar services, including those offered online, manufacturers, retailers, and service providers are responsible.
- E-commerce Return Policies: Under the legislation, e-commerce platforms must prominently publish their return and refund policies, and customers have the right to return items within a certain time frame if they are unsatisfied.
- False Advertising: Strict regulations are in place to prevent false advertising, which frequently influences e-commerce transactions.

3.4.2. Digital media ethics code and information technology intermediary guidelines, 2021:

These regulations, which were released under the Information Technology Act of 2000, are applicable to intermediaries, including e-commerce platforms, and they contain requirements meant to address consumer protection issues with regard to online content and transactions.

Key Requirements:

- Grievance Redressal process: Consumers who use e-commerce platforms must have access to a grievance redressal process, which makes it simpler for customers to report problems and look for solutions.
- Falsification of Goods: Regulations require sellers to refrain from misrepresenting their products or services, and intermediaries are obligated to take appropriate action in this regard.
- Counterfeit Products: E-commerce sites need to take action to stop the listing and sale of fake goods.
- Data Protection: Although these regulations do not only focus on consumer protection, they also highlight the importance of intermediaries protecting user privacy and data, which is crucial in the case of online transactions.
- Transparency in Sponsored material: Platforms must properly mark any adverts or sponsored material.
- Compliance Officer: Platforms must designate a Chief Compliance Officer, who is in charge of making sure that these regulations are followed.

Redress and Enforcement:

The consumer dispute redressal commissions created by the Consumer Protection Act of 2019 can help consumers who have problems with online transactions. These commissions have the authority to impose appropriate sanctions, such as compensation or refunds.

E-commerce sites that violate consumer protection laws and regulations may be subject to fines and legal action from customers or government regulators.

In India, a complicated legal area known as cybersecurity liability governs how people, businesses, and other entities are held accountable for cyberattacks, data breaches, and other cybersecurity-related incidents. Although India has not passed legislation specifically addressing cybersecurity responsibility, a number of other laws and regulations already in place provide the foundation for dealing with cybersecurity breaches and establishing accountability. In this article, we'll examine the idea of cybersecurity liability in India and the pertinent legal rules:

4. LEGAL PROVISIONS THAT ARE IMPORTANT FOR CYBERSECURITY LIABILITY:

4.1. 2000 Information Technology Act:

The main piece of legislation in India controlling cybersecurity and online transactions is the Information Technology Act (ITA). In order to meet new cybersecurity threats and breaches, it has been modified throughout time. The ITA's main cybersecurity liability clauses are as follows:

• Section 43A - Compensation for Data Breach: Under this provision, organisations and companies managing sensitive personal data are required to adopt appropriate security practises and procedures. If you don't, you could be held responsible and compensated for data breach victims.

• Section 66C - Identity Theft: This section addresses the crime of identity theft and outlines the consequences for those who

engage in it.

• Section 66D - Cheating by Personation: This section covers online cheating by personation and provides liability for those engaged in such actions, much like it does with identity theft.

• Section 72A - Penalty for Disclosure of Information in Breach of Contract - deals with the improper disclosure of sensitive personal data and establishes liability for those responsible.

4.2. The 2019 Personal Data Protection Act:

The Personal Data Protection Bill (PDPB), which had not yet become law at the time of my most recent knowledge update in September 2021, contains measures that potentially have major effects on cybersecurity liability. The legislation describes the duties of data fiduciaries (organisations handling personal data) and data processors, including their legal culpability for data breaches and failure to uphold data protection standards.

4.3.The IPC (Indian Penal Code):

There are provisions in the IPC that can be used to prosecute cybercrimes such hacking, internet fraud, and data theft. These laws create criminal responsibility and punishments for those who engage in cybercrime.

4.4.Banking rules and recommendations:

Banks and other financial institutions are subject to cybersecurity legislation and guidelines from the Reserve Bank of India (RBI). These regulations impose strict cybersecurity requirements on organisations and establish accountability for data breaches that damage customer information.

Responsibility and Repercussions: India's cyber security obligation may result in both civil and criminal repercussions:

• Civil Liability: Businesses and individuals may be held accountable in civil court for losses brought on by cybersecurity breaches, particularly if they neglected to take reasonable security precautions to safeguard sensitive information. Data breach victims may pursue compensation for their damages.

• Criminal Liability: Those who engage in cybercrimes including hacking, unauthorised access, and data theft may be subject to criminal penalties like jail time and fines.

• Regulatory Action: Organisations that violate cybersecurity and data protection laws may be subject to regulatory action from regulatory bodies like the RBI and the Data Protection Authority of India (should it be constituted under the PDPB).

6. CONCLUSION

Businesses must embrace digital transformation in the digital age as a strategic necessity rather than a side project. Those who do not run the risk of being left behind as the competitive environment keeps changing at an unprecedented rate. Digital transformation is about reinventing company models, processes, and consumer interactions in a digital-first environment, not just about technology. By doing this, businesses may seize new opportunities, promote innovation, and set themselves up for long-term success in the digital era. Businesses have never-before-seen prospects for innovation and growth thanks to digital transformation, but it also comes with a host of legal ramifications. Organisations need to work with legal specialists who are knowledgeable about technology and digital transformation to navigate this complex environment. In order to react to changing legal requirements, secure the benefits of digital transformation, and reduce legal risks, it is also crucial to maintain a proactive approach in monitoring legal developments in the digital sphere. Legal considerations must be incorporated into the digital transformation strategy strategically, not just as a matter of legal compliance.

In the age of digital transformation, data security and privacy are crucial, and organisations operating internationally, particularly those in India, must navigate a complex legal environment. Maintaining customer trust and avoiding legal ramifications related to data misuse require understanding and adhering to legislation like GDPR and the changing data privacy laws in India. To protect the interests of customers who engage in e-commerce and online transactions, India has established strong consumer protection laws and regulations. These laws cover a number of consumer rights facets, such as the right to information, the right to exchange items, and the right to protection from deceptive business practises. E-commerce platforms are expected to abide by these rules and offer consumers in India secure, dependable, and transparent online shopping experiences. In India, the area of cybersecurity liability is constantly changing, and new dangers are being addressed by changing legal frameworks. To reduce cybersecurity risks and potential liabilities, businesses and people should be aware of their duties and obligations under applicable laws and regulations. It is crucial for all stakeholders to be informed about changes in legislation and regulations as India develops its approach to cybersecurity and data protection in order to ensure compliance and data security.

REFERENCES

[1] Bélanger, F., & Crossler, R. E. (2019). Dealing with digital traces: Understanding protective behaviors on mobile devices. The Journal of Strategic Information Systems, 28(1), 34-49.

[2] Wieringa, J., Kannan, P. K., Ma, X., Reutterer, T., Risselada, H., & Skiera, B. (2021). Data analytics in a privacy-concerned world. Journal of Business Research, 122, 915-925.

[3] Khan, O., Daddi, T., & Iraldo, F. (2020). The role of dynamic capabilities in circular economy implementation and performance of companies. Corporate Social Responsibility and Environmental Management, 27(6), 3018-3033.

[4].Ji-fan Ren, S., Fosso Wamba, S., Akter, S., Dubey, R., & Childe, S. J. (2017). Modelling quality dynamics, business

value and firm performance in a big data analytics environment. International Journal of Production Research, 55(17), 5011-5026.

[5] Hussain, N., Rigoni, U., & Orij, R. P. (2018). Corporate governance and sustainability performance: Analysis of triple bottom line performance. Journal of business ethics, 149, 411-432.

[6] Cavusoglu, H., Cavusoglu, H., Son, J. Y., & Benbasat, I. (2015). Institutional pressures in security management: Direct and indirect influences on organizational investment in information security control resources. Information & Management, 52(4), 385-400.

[7] Verheyden, M., & Goeman, K. (2013). Does (company) size matter? Differences in social media usage for business purposes. Journal of Applied Quantitative Methods, 8(4).

[8] Raghupathi, V., & Raghupathi, W. (2019). Corporate sustainability reporting and disclosure on the web: An exploratory study. Information Resources Management Journal (IRMJ), 32(1), 1-27.

[9] Davenport, T., Guha, A., Grewal, D., & Bressgott, T. (2020). How artificial intelligence will change the future of marketing. Journal of the Academy of Marketing Science, 48, 24-42.