Canadian Journal of Marketing Research
ISSN: 0829-4836
https://canadian-jmr.com/index.php/cjmr

Research Article

Regulating Dark Patterns in Digital Marketing: A Comparative Review of Consumer Protection under the Digital Personal Data Protection Act, 2023 and the General Data Protection Regulation

Dr. Indra Daman Tiwari[1], Dr. Bishnanand Dubey[2], Dr. Kriti Singh[3] and Priyanshu Dennis Pascal[4]
[1]Assistant Professor, School of Law, T.S. Mishra University, Lucknow, Uttar Pradesh.
[2]Assistant Professor TMCLLS, Teerthanker Mahaveer University, Moradabad.
[3]Assistant Professor, School of Legal Studies, K R Mangalam University, Gurugram, Haryana.
[4]BTech (Masters of Science in Business Analytics), Wichita State University, Kansas, United States.

***Corresponding Author**
Dr. Indra Daman Tiwari (shivatiwari.lu@gmail.com)

Article History
Received: 15.02.2026
Accepted: 26.02.2026
Published: 20.03.2026

Abstract: The present paper is a critical analysis of the regulatory framework of the Digital Personal Data Protection Act, 2023, in India and the General Data Protection Regulation of the European Union in terms of combating the widespread dark patterns in digital marketing. These misleading designs of user interface take advantage of cognitive bias and push consumers toward unwanted behavior such as unnecessary purchase or subscriptions, compromising consumer autonomy in the digital market. The linked comparison below will outline the differences in conceptual approaches to the manipulation immersed in the dark patterns of these two unique legislative tools across the data protection and consumer rights domains. Particularly, it will discuss the extent of harm as defined in each framework and evaluating their effectiveness in addressing individual and social evil that emerges out of such manipulative acts. In addition, the review will examine the extent in which the various laws define the term dark patterns and in what implementation contexts the different aspects of the laws address more than a mere violation of direct data privacy and exploitative business activities. This involves a review of the legal framework of each jurisdiction as it attempts to resolve the natural tension between the business attitudes of maximizing customer data and ticket taking through targeted advertising, and the need to protect consumer privacy rights. The discussion will go further to establishing possible loopholes or whereby regulatory convergence may benefit global consumer protection against these emerging digital-based threats, given the fact that the availability of exploitation, as a central concept, tends to remain untheorized in consumer law.

Keywords: - Dark Patterns, Digital Marketing, Consumer Protection, DPDP Act 2023, GDPR, Data Privacy, Regulatory Comparison.

INTRODUCTION

Increase of e-commerce has created so-called dark patterns, harmful designs of user interfaces that can influence the choice of consumers who are affected by cognitive biases. Such consumer tricks, which include subscription traps, prepaid charges, and pre-set options usually exist in a regulatory grey zone and therefore they present a great difficulty in governance. Nevertheless, the inexact definition of the law and the fractured nature of the current frameworks, including those presented under the European Union Digital Services Act, Digital Markets Act and Data Act, help in creating a significant amount of legal ambiguity about how they apply to dark patterns. This regulatory loophole is increased by an extra level of complexity relating to the darker relationship between consumer protection laws and the data privacy laws which are likely to react to the same kind of manipulative design practices but through the lens of another jurisdiction and different subject matter. The power to safeguard consumer autonomy and data privacy is the critical feature of Digital Personal Data Protection Act, 2023, in India and the General Data Protection Regulation, in the European Union, concerning dark patterns in terms of device marketing in this paper. It will also be evaluated how these legislative frameworks will confront the natural contradiction here that is being presented by commercialization of consumer data and

profit maximizing targeted advertising that in most cases is dark patterns. The paper will also consider the role of these rules to differentiate between accepted forms of persuasive marketing and the manipulative dark patterns keeping in mind the fact that it is a complicated task to define what is deemed as unjust or deceptive behavior when no definite measurable harmful consequences are determined. This comparative text attempts to identify areas of overlap and difference between regulatory tools, and assess how far each model can go at sustaining manipulative possibilities of dark patterns and enable a dynamic future shaping of online marketing approaches. This kind of a comparative venture is necessary because there is a growing need to explicitly govern commercial practices that leverage consumer biases, such as in legislation that specifically prohibits the use of dark patterns in Internet platforms, such as Article 25 to Regulation 2022/2065 in the EU. The Digital Personal Data Protection Act, 2023, is the first attempt at an all-inclusive data protection framework in India, which is based on the EU and the US models but tailored to its own constitutional and socio-economic context. This act thus offers a worthwhile comparative prism to the obsolete GDPR, in assessing emerging global data protection standards and their consequences to consumer welfare versus misleading digital marketing legislation [1]. Specific defense mechanisms of both the DPDP Act and the GDPR that may be exploited to solve dark patterns by raising concerns about such aspects of the texts of the laws as consent, data minimisation, fair processing and other concerns of such practices, as well as deceptive commercial practices in general, will be delineated in this comparative analysis. This is through scrutinizing keenly the role played by the interpretative issues particularly around the issues of purported limitation of purpose and normalization of legitimate interest in the way these regulations are actually used in preventing the manipulation aspects of design [2]. In addition, the enforcement provisions and the bodies empowered to do so by each framework will also be analyzed in order to identify the extent to which the bodies in question are working in practise to curb and ensure the prosecution against the use of dark patterns by online marketers. The paper would also assess the potential of both the DPDP Act and the GDPR based on the jurisdictional scope and the extraterritorial impact both laws can have on the border dark pattern practices, which is critical looking at the globalized digital marketing [3]. This comparative study will, hence, provide details of the effectiveness of principle-based laws on data protection in preventing behavioral exploitation, in relation to scholarly criticism of the design of the laws, per se, in order to capture such covertly commercial practices. It will also fundamentally examine the sufficiency of the present state of DPDP Act in relation to data flows within the EU/EEA which is a central point of international data transfers. This point will determine whether the DPDP Act presents a sound constitution that can support the provision of the same level of protection as the GDPR, on the issue of controlling the dark patterns that exploit the personal data. These evaluations will make an analysis of the viability of these frameworks considering how such functions operate keeping in mind the pragmatic issues in terms of the detection and enforcement of violations of the dark patterns in various digital ecosystems. Statutory or interpretative proposals which may ameliorate the regulatory choke hold on dark patterns in either of the regimes will also be considered in the paper and the paper will discuss ways in which the current provisions might be refined or modified to offer a better protection against manipulative digital marketing practices.

2. Understanding Dark Patterns in Digital Marketing

Dark pattern Dark patterns refer to a particular aspect of manipulative design behavior exploiting cognitive biases to influence user behavior in a manner that is useful to service providers, often often at the expense of user autonomy and privacy. These design principles lead their users to the choices they otherwise would not make in a mild directive axis, and contain gimmicks such as hidden advertisements, forced subscriptions, and privacy-violating defaults. Continuing the example, dark design is strategically used on numerous online shopping stores to ensure unwanted purchases or subscriptions (including the addition of products to the cart), or even non-transparent unsubscribe. Similarly, websites tend to include consent banners, which arguably are easier to accept all cookies than privacy control or data processing disagreement, which can likewise be classified as despite an unfair commercial practice and are possibly subject to a challenge under GDPR. These false interfaces do not simply constitute an inconvenience, but a loss to consumer-confidence and even demonstrable damage by financial damage or even passive disclosure of personal data [4]. In fact, a study by computer scientists suggests that the use of dark patterns is mainly on the rise, and that they are specially designed to predatory effect and to traffick online consumers into unintended purchases or sensitive information. The most vulnerable groups, such as minors or less digital individuals, tend to be targeted by this manipulation, and that is why there are significant reasons to consider the urgency of a strong regulatory intervention. The difficulty of regulative governing frameworks such as the DPDP Act and GDPR is to comprehensively define and penalize these manipulative tasks that is less apparent and consequential, as in order to count as consent according to the regulations governing data protection, such permission should have to be an actualized and informed decision. In this way, the lack of truly free and informed consent, which is encouraged in many cases by dark patterns, makes the resulting data processing illegal in accordance with the GDPR and the forthcoming DPDP Act. This planned violation of user autonomy in design is not by chance but a calculated business solution to maximize its results, including the sale of the data, which usually results in functionality and/or worse user experience. By intentionally misleading the user with the use of dark patterns, this specific misuse and manipulation of user choice deliberately goes against the established idea of transparent and fair user data processing that is the core of extensive data protection laws. Such practices are often known as that as willful design dishonesty due to the manipulative nature of the activity and that the practice was discovered due to the conflict of interest involved with it, the desired outcome that the designer by a user [5]. This trick sets the manipulative practice invalid to the situation where the dark patterns mislead the consent particularly where all cookies accept buttons are unrealistically big, thereby going against

the consent form. The omnipresence of these bad-faith design tricks highlights the significance of regulatory operating systems to move beyond formalistic acquiescence to the evaluation of the substantive voluntariness and informed nature of user choice, especially in the context of design features that embrace vulnerability by design. Nevertheless, the inability of digital marketing techniques and customized algorithmic output to cease changing is also a significant obstacle to the regulatory bodies that continue to translate the customary paradigm of consumer security, typically founded on a sensible type of consumerism, into the solitary nature of the dark patterns [6].

THE REGULATORY LANDSCAPE OF DATA PROTECTION

The provisions of the GDPR and DPDP Act and their scope and suitability in various applications of dark patterns will be explored in the following sections [7]. This includes a detailed discussion of the legal interpretation and use of legal understanding of consent, data minimization, and fair processing to respond to deceptive interface designs. The enforcement procedures and called penalties contained in each of the frameworks and how they can deter the use of manipulative design practices will also be subjected to the same analysis [8]. Additionally, a review of available case law and regulatory guidance will help shedding some light on how the supervisory authorities operating in the EU and India have started to interpret and apply these regulations in relation to a dark pattern situation, giving an insight into the practical challenges or achievements in their application.

3.1. Overview of the General Data Protection Regulation (GDPR)

Enacted in 2016 and becoming effectual since 2018, the GDPR is a general lawful foundation of personal data processing in the European Union developed by considering the fact that an individual is at the centre of the needs of personal data protection that represents his fundamental right. It has strict provisions on consent requirement, data subject rights, and data controller and data processor accountability, which have had serious impact on data protection standards globally. Its extra-territoriality implies that organizations that store the data of the EU nationals abroad cannot forego it, thus establishing a standard in the regulation of data across the globe. Importantly, wide-ranging and conceptual provisions of the GDPR have prompted numerous debates in the field of law about the effectiveness of the regulation in the face of behavioral manipulation such as dark patterns against which the regulation was not even meant. However, the regulators have understood the principles of fairness and transparency under GDPR to refer to interfaces that are created to tempt or deceive a user into agreeing to have data processed about them. The GDPR in particular considers such information, related to an identified or identifiable natural person, as personal data, and governs the entire activity of processing personal data carried out by a data controller or processor that delivers goods or services to, or surveils the behavior of, people resident within the EU. The strong consent conditions being stipulated by the GDPR, in terms of unambiguous, specific, informed and freely verbative consent, take a direct toll on the effectiveness of the dark patterns that are used to bypass user autonomy. This framework therefore subjects organisations to ensure there is express user consent prior to gathering any data, offer clear and detailed information about data processing, and allow user to make their own informed consent whether to allow or reject the process of data collection, with pre-comparing boxes or lack thereof must certainly disqualified as compiled consent.

3.2. Key Principles and Provisions of the GDPR Relevant to Dark Patterns

The guiding principles of the mitigation of the dark patterns according to the GDPR comprise the principles of consent, data minimization, and the rights of a data subject, namely the right to information and the right to object to processing. Particularly, the consent under Article 4 of the GDPR is defined as any indication of the wishes of the data subject as it signifies consent to the processing of the personal data voluntarily, precisely, duly and expressly, if it is possible to determine it through a declaration or a clear affirmative act. Such definition implicitly excludes consent that could have been secured by deceptive design features; since the procedure will result in violation of the freely given and informed requirements of consent that the regulation imposes. The direct limitation of dark patterns in the EU legislation, the Digital Services Act, which specifically addresses interfaces to deceive consent, also highlights the trend into which the regulation aims to ban such manipulative designs. Besides, the transparency characteristic of the GDPR assumes that data that is reported to the subjects has to be very brief, easy to comprehend, and devoid of any form of misleading information that can confuse the essence of processing data. This is done by ensuring that consent requests are visually distinct with regards to other features of an interface, and by ensuring that pre-checked boxes and inactivity are not found to amount to consent. Also, the principle of data minimization, enshrined in Article 5 of the GDPR, stipulates that data deemed to be essential to a certain purpose ought to be processed, which directly conflicts with dark patterns that force users to disclose too much personal information, as in a basic online shopping operation, which may demand occupation or income details.

3.3. Introduction to the Digital Personal Data Protection Act, 2023 (DPDPA)

Although parallels to the GDPR are made by the DPDP Act, the Indian legal and digital environment will have a specific regulatory frame, and there are new data fiduciaries and processors standards in the country. The aim of the legislation is to protect personal data by establishing obligations on these entities that receive such data and gives people more authority concerning their information, especially in the framework of digital marketing activities where dark patterns are common. The Act, then, intends to reduce the negative impact of manipulative design by means of provisions prescribing clear

consent and openness in the treatment of data. Particularly, Section 6 of DPDP Act, 2023, follows the GDPR in that the consent must be freely given, informed, and unambiguous, thus implicitly prohibiting consent obtained under false design recognition features. The proposed compatibility with the strict consent provisions of the GDPR highlights a worldwide move towards uniting eclectic data protection principles in an effort to guarantee the independence of the user and to discourage manipulation of online relations. Therefore, the DPDP Act opens such mechanisms as explicit and informed consent where it is essential to provide an explanation of the purpose, scope, and the period of processing of data, specific consent and the ability to take it away [9]. Extremely harsh penalties also apply in the event of non-compliance, which attempts to provide a strong deterrent to players who subvert user choice using dark patterns. Besides, DPDP Act, 2023, based on the postulates of the Puttaswamy case, enhances privacy as an essential right and represents a legal pillar on the foundation of which individuals could master control over the personal information that they possess.

4. Comparative Analysis of GDPR and DPDPA in Regulating Dark Patterns

The following part will critically analyze how the concept of consent based on the conceptualization provided by the GDPR and the DPDP Act interact (or are claimed to interact) with one another; how differences in definitions and conditions/requirements of the two could influence their respective efficacy in relying upon the commission of the acts of dark patterns automating user assent [10]. It will also explore the extent of data subject rights in each rate and how these rights can be used to question or to correct consent using false fronts bearing in mind that the DPDPA does not report all rights that the GDPR includes. The mechanisms used to enforce it will also be evaluated in detail, such as the authority of the Data Protection Board in the DPDPA and the supervision bodies in the GDPR, to determine their ability to impose penalties on organizations that use dark patterns. Lastly, this part will also evaluate the transparency requirements placed upon data fiduciaries by both laws and determine their usefulness in helping to avoid dark patterns that hide the data processing process or distort user decisions.

4.1. Scope and Applicability

As the GDPR has wide extraterritorial ransom, and applies to any entity that processes the personal data of the EU residents, the magnitude of the DPPA largely relates to the data processing in India. Nevertheless, despite this geographical boundary, the DPDP Act delineates such principles as consent-based processing and individual rights, which are also relevant in the GDPR, with the significant difference in implementation and strict limitations, including the lack of clear conditions concerning sensitive and critical types of data and strong state surveillance restrictions, which are presented in the GDPR. Moreover, the definition of personal data under the DPDPA does not as of today cover every type of data, as compared to the full scope of the framework used in the GDPR, which may restrict its applicability to new modes of data misuse through the dark patterns. Individually, as an example, the DPDPA does not even specifically distinguish between personal data as sensitive and non-sensitive, which may have an impact on the degree of protection provided against subtle dark patterns [11]. Such divergence can result in differences in receiving data privacy violation, especially one caused by advanced dark patterns, differently in different jurisdictions. Additionally, given that the DPDP Act does not sub-categorize the definition and understanding of personal data, the inclusion only of a single definition may inadvertently allow some data-driven dark patterns to act in a regulatory grey box relative to the GDPR sub-categorization of sensitive data.

4.2. Definitions and Recognition of Dark Patterns

Although both the GDPR and the DPDPA do not specify the concept of dark patterns, both regulations reflect the mentioned ways of misinformation in their provisions on consent, transparency, and the right over data. But their oblique strategies do require encoding activities that render these broad rules applicable to limited manipulative design strategies. The latter interpretive problem is made especially obvious in the DPDPA, where, contrary to the GDPR, the various data types are not classified fully, so the evaluation of the harm caused by the dark patterns manipulating various types of personal data may turn out to be a difficult endeavor. Such a difference comes to the fore when we think about the ways in which dark patterns could misuse sensitive information because failure to provide explicit protection to such information under the DPDPA may expose people to more sophisticated versions of manipulation. Further, sensitive personal data is not explicitly defined under the DPDPA and a Data Protection Impact Assessment is not required to be conducted on every data fiduciary who handles health data, unlike the more specific approach to data classification and risk-assessment found in the GDPR. Varried definition accuracy and differing approaches to risk measurement might result in uneven application of regulatory controls in addressing dark patterns, particularly those involving subtle manipulation of the psyche in comparison to actual data breaches. Thus, this classification difference implies that the DPDPA does not require a data protection impact assessment to be conducted by significant data fiduciaries when they process sensitive personal data, which is an essential requirement under the GDPR in order to reduce privacy risk.

4.3. Consent Mechanisms and Withdrawal of Consent

These mechanisms can only be effective under the condition of specific guidelines on what will be considered truly informed and free and given consent, and here regulators are still working on establishing the interpretations under the influence of ever more complex dark patterns. This is made more complex by different ways of diagnosing consumer vulnerability across different jurisdictions, some legal systems, such as the Unfair Commercial Practices Directive in the EU, admit that the vulnerability of consumers is dynamic and circumstantial, and still, provides little guidance on judicial

review of the situation among shifting dark patterns. Although in the U.S. deceptive and unfair practices are typically outlawed in Section 5 of the Federal Trade Commission Act, certain laws, such as the California Privacy Rights Act, directly discuss dark patterns, which are defined as interfaces aimed to undermine user autonomy. However, an explicit definition is still missing in the GDPR and the DPDPA, and the use of general data protection principles is required to draw conclusions about any prohibitions on manipulative elements of design.

4.4. Data Protection Principles and Dark Patterns (e.g., Transparency, Fairness, Accountability)

The core principles of data protection (limitating the purpose, prudence of data, accountability, etc.) are directly violated by covert nature of data gathering and processing involved in the dark patterns. Such design patterns take advantage of cognitive biases to encourage the user to make a decision advantageous to the data fiduciary and often remove the need to collect more personal data than is strictly required based on the stated purpose. This violation negates the rights of the user to decide on their personal data and questions the integrity of consent processes, upon which both the GDPR and the DPDPA are based. A striking illustration of this violation is found in the areas of consent management, with just a exceptional portion of the extensions truly satisfying the European criteria of consent, and dark patterns and covert consent being prevalent [12]. This is made even more difficult by the dynamic and situational character of the dark patterns and how they tend to evolve with the user actions and technology adaptation, making it challenging to define and implement ex ante legal definitions. This implies that regulatory authorities must adopt a process of constant interpretation to determine that isolating and accepting manipulative design as being in accordance with fundamental principles of data protection.

4.5. Consumer Rights and Enforcement Mechanisms

Consumer rights in the area of dark patterns are enforced with significantly different mechanisms depending on jurisdiction due to diverse legal and regulatory traditions. An example is that when the GDPR offers to impose large administrative fines on non-compliance, the DPDPA gives follow-up on a list of penalties that, even though they are large, may vary in their practice and scope, especially with regard to new manifestations of digital manipulations [13]. In addition, the possibility of such enforcement mechanisms frequently is disputed by the cross-national character of digital marketing, as well as by the difficulty of determining malicious intent based on manipulative design and, consequently, limiting cooperation between countries and recourse to the law in the context of a victim. This exemplifies the need of uniform international regulatory measures and effective interpretative directives to successfully combat the emergent frontier in dark patterns in digital marketing. Moreover, the maliciousness of dark patterns, which tend to manipulate users with indirect hints and manipulative design, requires experimental studies to accurately measure that manipulative effect and find the means of creating such mechanisms more related to transparency. These solutions must not merely be based on the use of punitive action but also with a focus on international collaboration, transparent regulations and greater digital literacy in order to allow users resist manipulative practices.

4.6. Penalties and Sanctions for Non-Compliance

The GDPR and the DPDPA both specify the schemes of imposing penalties and sanctions, although their policies differ concerning the maximum amount of the fines, the conditions of their application, and the authorities who are authorized to carry them through. Namely, the GDPR provides penalties of up to EUR20 million or 4% of annual global turnover, whichever is greater, in case of serious offenses, and the DPDPA, in its turn, adheres to a different scale and even different hierarchy of enforcement. This inequality also carries over to the amount of possible criminal penalties, some European regimes allowing sentences to be imposed on managerial roles dealing with non-adherence, which is not directly reflected in all consumer protection laws. The strong enforcement structures of GDPR, especially its high financial fines, has been proven to be effective in holding organisations to the task of breaching data privacy, and has had an impact on changing the data culture of corporations. Such a strong enforcement, though, may not be easy to impose because of epistemic difficulties inherent in knowing completely what algorithmic operations and design do in order to demonstrate non-compliance. This has frequently prompted the use of competition law redress, particularly in cases where the enforcement of data protection does not adequately prevent the actions of large digital platforms that engage in bundling of consent practices [14]. However, no cases of extensive damages claims are being presented in GDPR case law about the dark patterns, meaning that the full scope of the magnitude of damage is not being addressed, especially along non-quantifiable aspects. Thus, the issue of non-pecuniary damage evaluation and measurement caused by the dark patterns should be further explored to provide the methodology to enhance the compensatory part of data protection laws.

5. Challenges and Opportunities in Regulating Dark Patterns

The ubiquitous and developing reality of dark patterns poses tough riddles to the regulators who must keep up with the changing and transforming technology and the ever-unstable ways and strategies of digital manipulation. The first one is that it lacks a universal ontology of dark patterns and, as a result, becomes hard to deal with in different digital contexts and settings. It is unclear as a conceptual condition and hence cannot propose any definite legal specifications and enforcement policies, particularly in establishing the boundaries between persuasive design and manipulative dark patterns [15]. Moreover, the relative financial benefits that the execution of dark patterns can generate, combined with the comparatively small penalties that are provided by different jurisdictions decrease the discouragement power of the punishment, particularly since the abilities provided by artificial intelligence to develop more innovative and efficient

manipulative tactics are quite effective.

5.1. Identification and Classification Challenges

Subtle distinction between accepted persuasive design best practices and manipulative dark patterns may still pose a significant challenge to overcome, as it might demand context research on user intent, cognitive distortions minimized, and the negative impact on independent decision-making. What further makes the matter complex is the fact that there are no common ethical structures in the industry and thus it is hard to determine the matter of acceptable design practice. To make things worse, empirical studies would be essential in the ability to differentiate unintentional design flaws and willful dark patterns, since some manipulative methods can still remain in place notwithstanding their factual elimination, a concept known as effect survival [8]. The existing approaches to identifying and categorizing dark patterns tend to inadequately represent their richness and complexity and poses the risk of undergoing influencing biases that might lead to poor external validity of the research and the efficacy of applying regulations. The lack thereof is most clearly apparent by the fact that a comprehensive taxonomy that would cover the different sources and forms of dark patterns, thereby facilitating standard investigation and intervention activities, does not exist. Such lack of a differentiated way of defining it becomes an important hindrance to the creation of effective regulatory responses because the lack of form in the dark patterns makes it harder to draw clear lines between what constitutes normal user experience optimization and what can be considered an ethically dubious effort to guide people into the actions they desire [16].

5.2. Jurisdictional Issues and Cross-Border Enforcement

The transnational nature of online platforms also intensifies regulatory pressures, with behaviors that may form dark patterns in a particular jurisdiction potentially affecting customers across multiple jurisdictions, leading to complex international cooperation and harmonizing legal regulation to achieve effective enforcement across borders. Since regulatory power is frequently divided across national borders, the paradox of accountability regularly occurs, with several frameworks all applying at any given time but no reliable oversight being made. Such jurisdictional obscurity is especially troublesome considering the fact that most legal regimes at the national level do not have the particular legislative tools to directly govern dark patterns, thus making enforcing it on the actors that have established their presence on a global scale very difficult. In addition, the constantly shifting and changing quality of digital interfaces ensures that regulation is usually playing catch-up, so it differs in terms of whether it is feasible to legislate against practices that are continually being optimised or are freshly introduced. This difficulty is accentuated by the fact the dark patterns in themselves are often modeled so they are harmless to the user, such that they can also impair generating complaints by the user as well as enforcement by the regulator. The absence of a unified international strategy also contributes to poor preventing, with disjointed regulation and difference in legal interpretations leaving low points in prevention that can be used by multinational companies.

5.3. Technological Evolution and Adaptive Regulation

The pace of technological change, in particular, the new stage of high-level artificial intelligence, is continuously imposing new forms of dark patterns onto the economy, new of which must be not only active but also naturally adaptable to new approaches to manipulation, which are presented by digital methods. It demands the reactive enforcement to be changed to anticipatory governance systems, which will react to the unforeseen digital harms and offer long-term consumer protection. The transnational and complicate nature of transformative technologies poses significant problems to governments in the implementation of regulations across digital borders, and jurisdictional regulation is a complicated issue. What strengthens this further is the fact that a majority of the digital systems are being cooked in one particular jurisdiction and executed on a global platform and this gives rise to ambiguity concerning the legal norms and processes to be applied and enforced as law [17]. The complexity of this dynamic often results in a regulation vacuum and insufficient accountability framework with the decision of what risk will arise after the deployment is completed being unclear. The crunch-timing issue in which law-making institutions are constrained to remain within the rapid development in technology, or the time lag involved to create the effect of a regulation is traditionally compensated by the publication of an obsolete regulation.

5.4. Balancing Innovation with Consumer Protection

This must be balanced and is coming across as a tight spot more so given the fact that excessive control can result in the elimination of any positive technological advancements and economic growth thus failure to control results in digital abuse in a vast scale. Value systems are thus to be responsive to the innovation where ethically driven principles ought to be considered in conceptualization of the innovation, rather than simply removal of some manipulative drills, which would also enable self- revolved action in the industry. To an extreme, however, a governance paradox is likely to sabotage the process of establishing such frameworks, in which, the incentive of innovation is invariably likely to come into conflict with the requirement to possess a good ethical standards and good degree of control in particular with establishment of multinational companies. This paradox was also complicated by the black box nature of various advanced AI systems since it is challenging to establish uniform guidelines of governing that explores the trade-off between innovation and ethical accountability. It could be especially relevant in the aftermath of the potential bluewashing when the organizations could carry out strictly superficial cases of ethical activities as a way of getting away with actual regulatory scrutiny [18]. The rapid evolution of AI also introduces significant challenges for regulators in maintaining market integrity and ensuring

consumer protection within financial sectors.

CONCLUSION

The review has rigorously dealt with the complex issues of controlling dark patterns in digital marketing, especially in the context of the Digital Personal Data Protection Act, 2023, and the General Data Protection Regulation. The discussion highlights the long-standing challenges in converting ethical standards into legally binding regulatory models, especially with the fast development of artificial intelligence and data-driven marketing. Despite their importance, both the DPDPA and the GDPR face the same issue of regulation frameworks trying to keep up with the increasingly rapid technological development. Particularly, the growing use of AI in personalized marketing turns up to the personalization-privacy paradox when consumers prefer customized attention, but raise concerns regarding the misuse of their data and the lack of transparency. This paradox is additionally aggravated by the fact that AI algorithms are opaque, and it is almost impossible to trace the consequences of using the data, thus, provoking a challenge toward conventional models of informed consent. This concern is of particular concern where real time monitoring, and the Internet of Things are common, and there is an urgent requirement of moral regulation on how user behavior is tracked and how data dignity is maintained within the life cycle of data. Moreover, the nature of most AI-driven systems is complex and black box in nature, which makes it extremely hard to determine the decision-making process, making transparency and accountability very challenging, which are the pillars of a strong data protection regime such as the GDPR. This obscurity also helps to make it considerably harder to detect and punish manipulative dark patterns that are commonly integrated into complex algorithmic processes aimed at exploiting cognitive biases. Besides, the ineffectiveness of such policies is frequently caused by insufficient definitions of such terms as dark patterns and the following issues of their enforcement since, often, they are vague and changeable, working not within the boundaries of laws, but on the margin of them. This uncertainty is also compounded with the vagueness of the existing data protection legislation, which, although accepted as all-encompassing, may cause some confusion in the legal context and may suppress appropriate deployment. The difference between the ideals of regulation and the real characteristics of introducing transparency and consent in the applications of AI-based marketing just keeps increasing, even though the interactive consent mechanisms are being enhanced.

REFERENCES

1. Jha, A. K. “The Changing Face of the Data Protection Laws: From India’s IT Act to Global Privacy Standards.” *African Journal of Biomedical Research*, Oct. 2024, p. 2004. https://doi.org/10.53555/ajbr.v27i1s.1767.
2. Naithani, P. “Analysis of India’s Digital Personal Data Protection Act, 2023.” *International Journal of Law and Management*, vol. 67, no. 5, July 2024, p. 543. https://doi.org/10.1108/ijlma-05-2024-0174.
3. Yadav, V. “Crossing Borders: Comparative Perspectives on Data Protection Laws in India, the EU, and the US.” *Journal on Development of Intellectual Property and Research*, vol. 1, no. 2, July 2025, p. 38. https://doi.org/10.64618/faasre69.
4. Kaur, S., and V. Kumar. “Consumer Protection and Deep Fakes - Assessing the Rights and Remedies for Victims in India.” *International Journal for Research in Applied Science and Engineering Technology*, vol. 12, no. 4, Apr. 2024, p. 1032. https://doi.org/10.22214/ijraset.2024.59830.
5. Chalhoub, G., and I. Fléchais. “Data Protection at a Discount: Investigating the UX of Data Protection from User, Designer, and Business Leader Perspectives.” *Proceedings of the ACM on Human-Computer Interaction*, vol. 6, Nov. 2022, p. 1. https://doi.org/10.1145/3555537.
6. Yi, W., and Z. Li. “Mapping the Scholarship of Dark Pattern Regulation: A Systematic Review of Concepts, Regulatory Paradigms, and Solutions from an Interdisciplinary Perspective.” *arXiv*, Cornell University, 14 July 2024. https://doi.org/10.48550/arxiv.2407.10340.
7. Conca, S. D. “The Present Looks Nothing like the Jetsons: Deceptive Design in Virtual Assistants and the Protection of the Rights of Users.” *Computer Law & Security Review*, vol. 51, Sept. 2023, p. 105866. https://doi.org/10.1016/j.clsr.2023.105866.
8. Gray, C. M., et al. “Dark Patterns and the Legal Requirements of Consent Banners: An Interaction Criticism Perspective.” May 2021, p. 1. https://doi.org/10.1145/3411764.3445779.
9. Kumar, V. “Data Privacy and Consent in E-Commerce Transactions: A Legal Examination of the Digital Personal Data Protection Act, 2023 and Its Impact on Online Consumers.” *International Journal of Applied Research*, vol. 11, no. 10, Jan. 2025, p. 388. https://doi.org/10.22271/allresearch.2025.v11.i10e.12969.
10. Chaurasiya, V. R. “Consent Mechanisms under the Digital Personal Data Protection Act, 2023: A Comparative Legal Analysis with GDPR and CCPA/CPRA.” *LawFoyer International Journal of Doctrinal Legal Research*, vol. 3, no. 2, June 2025, p. 517. https://doi.org/10.70183/lijdlr.2025.v03.61.
11. Singh, K. K. “India’s Legal and Policy Approach to Personal Data Protection and Cross-Border Data Transfer: A Critical Study with Special Reference to Health Data.” *Perspectives in Law, Business and Innovation*, Springer Nature, 2024, p. 219. https://doi.org/10.1007/978-981-97-9983-1_11.
12. Nouwens, M., et al. “Dark Patterns after the GDPR: Scraping Consent Pop-ups and Demonstrating Their Influence.” Apr. 2020, p. 1. https://doi.org/10.1145/3313831.3376321.
13. Fassiaux, S. “Preserving Consumer Autonomy through European Union Regulation of Artificial Intelligence: A

Long-Term Approach." *European Journal of Risk Regulation*, vol. 14, no. 4, Aug. 2023, p. 710. https://doi.org/10.1017/err.2023.58.

14. Kerber, W., and K. K. Zolna. "The German Facebook Case: The Law and Economics of the Relationship between Competition and Data Protection Law." *European Journal of Law and Economics*, vol. 54, no. 2, Mar. 2022, p. 217. https://doi.org/10.1007/s10657-022-09727-8.
15. Brenncke, M. "Regulating Dark Patterns." *arXiv*, Cornell University, Sept. 2023. https://doi.org/10.48550/arxiv.2310.00340.
16. Li, M., et al. "A Comprehensive Study on Dark Patterns." *arXiv*, Cornell University, Dec. 2024. https://doi.org/10.48550/arxiv.2412.09147.
17. Chaudhary, D. "The Ethics of AI in Pricing: Fairness, Transparency, and Accountability." *International Journal of Computational and Experimental Science and Engineering*, vol. 11, no. 3, Sept. 2025. https://doi.org/10.22399/ijcesen.3949.
18. Hermann, E., G. Y. Williams, and S. Puntoni. "Deploying Artificial Intelligence in Services to Aid Vulnerable Consumers." *Journal of the Academy of Marketing Science*, vol. 52, no. 5, Nov. 2023, p. 1431. https://doi.org/10.1007/s11747-023-00986-8.