INTERNATIONAL JOURNAL OF NOVEL RESEARCH AND DEVELOPMENT (IJNRD)
© 2026 IJNRD | Volume 11, Issue 3, March 2026 | ISSN: 2456-4184 | IJNRD.ORG

Systematic review for analyzing the Dark Patterns International Regulations, Guidelines and India's aligned actions

[1]Dr. Kanti Singh Sangher, [2]Arjun, [3]Dr. Mary Jacintha M

[1]Scientist-E, [2]Software Developer, [3]Scientist-F
[1,2,3]Eduction and Training,
[1,2,3]Centre for Development of Advanced Computing, Noida, India

Abstract: Dark patterns are a representation of design strategies in digital interfaces that 'gently' persuade users to perform actions that were not originally in their goals, such as sharing personal information or making transactions. Although this may provide benefits to the company in the short term, it may also create problems in the long term. In the long term, a company's reputation may suffer, and there may even be legal consequences. Organizations that continue to practice dark patterns are in an even tighter spot as regulations are being strictly imposed due to increased awareness of this issue. Approximately 25% of Internet users are exposed to black patterns, and this issue has caught the attention of governments all over the world, leading to the formulation of new regulations regarding this issue. From the recommendations of guidelines and directives issued regarding this issue, it is clear that there are different strategies to fight this problem, depending on the country's guidelines and pattern types. However, there appears to be a lack of consistent enforcement of legislation designed to counter deceptive design patterns. The ethical application of user experience design is becoming more and more important for upholding user trust and adhering to new rules as digital interfaces continue to develop. In this research paper comparative analysis of various countries actions taken in the form of regulations, guidelines, acts and best practices are covered. India's action to handle the dark patterns-based applications have been also covered, and how these legal measures can take shape to make ethical user interface design practices.

Index Terms **– Dark Pattern, Regulation, Guidelines, Law, Privacy**

I.INTRODUCTION

Dark patterns are deceptive design techniques used in digital interfaces to trick people into making decisions they may not have consciously chosen. These tactics can lead users to unintentionally sign up for services, purchase items they didn't intend to buy, or share personal information without fully understanding the consequences. While these strategies might offer short-term gains in sales, sign ups, or data collection, they can result in significant long-term harm to both users and businesses Dark patterns have far-reaching negative repercussions, most especially in undermining a firm's reputation and eroding consumer trust. In the current digital environment, when user experiences are quickly disseminated via social media and other online platforms, misleading or annoying encounters can quickly lead to public censure and damage to a brand's reputation. The users tend to lose faith in the company, and this often results in a loss of clients. The General Data Protection Regulation of the European Union, the California Consumer Privacy Act of the United States, the guidelines of the South Korean Fair-Trade Commission, and the regulations of the U.S. Federal Trade Commission are some of the legal measures taken to avoid such situations. They are designed to protect the data of their citizens from such practices. They prohibit such practices and insist on transparency, consent, and fair treatment. This means that companies must always deal fairly and transparently with their users. More than any law, it is these principles that are likely to undermine the foundation of trust upon which the company must build its long-term success.

II. LITERATURE REVIEW

Several nations have introduced laws and restrictions regarding dark patterns, and several organizations have provided specific guidelines and suggestions. These laws and guidelines have been introduced by several organizations in several nations to protect customers from unfair practices of dark patterns. The European Data Protection Board Guidelines for social media platform design has been made available by EDPB and member states of the European Union (EU) [4]. This article has provided samples and divided dark patterns into fifteen subgroups and six main categories. It has brought to the reader's attention specific legal principles in UI design, which are lawfulness, justice, transparency, purpose limitation, and data minimization [5]. These guidelines have been made to cooperate with the enforcement of GDPR 2016 for handling any violation of dark patterns [6]. Federal Trade Commission Study discusses the United States FTC and highlights specific findings of the workshop "Bringing Dark Patterns to Light" and studies [7].

By providing helpful guidance, the FTC helps companies improve their user experience. Four types of dark patterns in websites and apps that are emerging in the internet industry have been discussed in the study. There are two key points mentioned in the study: Firstly, it is mentioned that organizations that use dark patterns in their business will face consequences from the FTC, which works for the protection of customers. Secondly, organizations that use dark patterns in their business are always under scrutiny.
The Korean Fair-Trade Commission is developing regulations to regulate dark patterns on the internet. This initiative involves the Korean FTC, the Personal Information Protection Commission (PIPC), and the Korean Communication Commission (KCC). The report lists 19 distinct kinds of dark patterns, classifies them into 4 major groups, and offers recommendations for each [8].

The KFTC has established a penalty for companies that violate these regulations, with fines determined by the total sales of the company for that year. Through India's Central Consumer Protection Authority (CCPA). It says that participating in any kind of dark pattern practice is forbidden by the principles against dark patterns for anyone, including platforms. Certain categories of forbidden dark patterns have been listed in the study. Dark patterns have been divided into thirteen categories by the paper, which also includes pertinent instances [9]. The Asia Internet Coalition (AIC) provided reviews and recommendations, which were then used to establish these dark pattern guidelines [10].

The Consumer Protection Act of 2019 includes the dark pattern requirements, and compliance with the rules will result in penalties in addition to the Act's enforcement. California Consumer Privacy Act has adopted laws under the CCPA 2018 to suppress the usage of dark patterns. Dark patterns that significantly impact a consumer's decision to opt out of schemes that benefit firms or entities are prohibited by the California Civil Process Act (CCPA) [11,12,13]. Additionally, they have established a few instances of these "dark patterns," such as the use of ambiguous language, such as double negatives, among others. Businesses or organizations who have broken these rules are allowed to make improvements to their website or app for 30 days after the violation. Under the CCPA, there will be civil penalties for failing to make the necessary modifications [14].

III. RESULT AND DISCUSSION

The primary focus of this part is a thorough analysis of the documents that make up the guidelines. The Central Consumer Protection Authority (CCPA) for India, the European Data Protection Board (EDPB) for the European Union, the Korean Federal Trade Commission (KFTC) for South Korea, the Federal Trade Commission (FTC) for the United States, and the California Consumer Privacy Act (CCPA) are the authorities that have provided these guidelines [17]. Dark pattern guidelines available worldwide with their enforcement mechanisms are shown in the Table 1.

Table 1 Dark Pattern Guidelines

Guidelines/ Laws	Definition of Dark Pattern	Transparency Requirements	Enforcement Mechanism
1. European Data Protection Board. 2.Chapter 2&3, General Data Protection Regulation (2016)	Actions frequently violating users' rights to data protection by tricking or manipulating their decisions.	Demands unequivocal, explicit, well informed consent before data is processed. Consent must be easily withdrawn by users.	Penalty of up to €20 million, or 4% of global income, whichever is higher. Compliant is enforced by regulatory agencies. [15]
1. Federal Trade Commission. 2.Section 5, FTC Act, 2004	unethical or dishonest business practices that deceive clients or capitalize on their behavioral prejudices to produce harm, unanticipated outcomes.	To prevent fraud, disclosures must be made in a clear and noticeable manner. It is required that all aspects of service, price, and data gathering be transparent.	Enforcement through fines, injunctions, and corrective actions. The FTC can sue companies that violate the rules. [16].
1. Korean Fair-Trade Commission. 2. Personal Information Protection Act (PIPA), 2011 & e-Commerce Act, 2019	Practices that trick or coerce users into sharing more data than necessary or making unwanted purchases, violating consumer rights.	It is necessary to be transparent while collecting and using personal data. Consent needs to be explicit and knowledgeable.	Administrative fines up to 3% of total sales.
1. Central Consumer Protection Authority (India). 2. Section 18, Consumer Protection Act, 2019	Commercial practices that manipulate consumer decisions through misleading or deceptive information or coercive tactics.	Advertisements and terms must be clear, accurate, and not misleading. Consent and opt-out options must be straight forward.	Enforcement Mechanism Imprisonment of 6 months or a fine of up to INR 2 million (USD 24k) or both

IV. FINDING AND COMPARATIVE ANALYSIS RESEARCH

A detailed analysis is shown in the Table 2, dark patterns are prevalent across countries, and the country wise guidelines, outcomes, identified gaps, and resulting challenges are systematically presented in the table.

Table 2 Comparative Analysis Research

Country	Research Paper/Guidelines	Outcome & Gapes identified	Result's & challenges
United States	Dark Patterns at Scale, 2020. [18]	Explains the usefulness of dark patterns, the shopping sector, and automated methods for spotting dark patterns on a wide range of websites. The study may have missed dark tendencies common to other businesses because it focusses mostly on retail websites	Although the automated detection method greatly enhances large-scale identification, it is not subject to regulatory enforcement. Future developments should incorporate findings into consumer protection laws and broaden the investigation to other sectors (such as social media and financial services).
European Union	The Impact of GDPR on Dark Patterns, 2021. [19]	Examines how GDPR can be used to mitigate dark patterns and offers suggestions for additional regulatory improvements. Primarily on GDPR; lacks a more comprehensive understanding of how various EU member states handle dark patterns on an individual basis.	Especially in terms of cookie consent mechanisms, it has managed to control manipulative practices within the EU territory. Nevertheless, there is a need to develop a more unified enforcement structure across all participating countries. Consumer protection can be enhanced through the incorporation of GDPR principles into algorithmic transparency and AI-driven dark patterns.
France	The Effect of Design Patterns on (Present and Future) Cookie Consent Decisions. 2022. [20]	As indicated in the study, permission ad design significantly influences cookie acceptance. "Bright patterns" and behavioral levers increase the user's propensity to reject, enabling them to act in a more informed way regarding their privacy. Since it is conducted in a controlled environment and only encompasses e-commerce websites, it is not possible to completely generalize the results to all kinds of websites.	"Bright Patterns" has been emphasized by France, and it is seen as a viable solution to dark patterns. More detailed information can be obtained through more research using multiple digital mediums such as social media and mobile applications. The results should be included in more stringent consent laws.
Canada	1. Privacy Dark Patterns: A Case for Regulatory Reform in Canada, 2023. [21] 2. Approaches to Regulating Privacy Dark Patterns, 2024 [22].	1. Canadian laws regarding privacy in controlling dark patterns of privacy, ideas regarding policies and regulations. More emphasis on privacy does not discuss dark patterns of privacy except those that are related to it. 2. The study emphasizes that Canada should have stronger privacy regulations like those in CCPA and GDPR. Bill C-27 is a good change, but it is still not sufficient to protect consumers effectively. Approaches at the legislative level are needed, complemented by technological support and public education in order to sensitize users about manipulative designs. Without these dual approaches, privacy in a digital world would be unthinkable.	With Bill C-27, Canada has made progress, but its enforcement systems are still insufficient. Consumer protection can be improved by enforcing stricter penalties, extending oversight to non-privacy dark patterns (such as misleading user interface practices), and using AI driven monitoring technologies. Campaigns for general awareness ought to be launched as well.
South Korea	South Korea's PIPA and Dark Patterns, 2022.	Focuses on current enforcement actions and analyses how South Korea's Personal Information Protection Act has reduced deceptive patterns. Little focus on cross industry analysis; mainly cantered on online shopping platforms	Although PIPA has effectively addressed privacy related dark patterns, there is still a gap in its limited application in other businesses. Its efficacy can be increased by expanding rules to include financial services, mobile apps, and new manipulative strategies powered by AI.

India	Guidelines for Prevention of Misleading Advertisements and Endorsements for Misleading Advertisements, 2022 [23].	The CCPA, under Section 10 of the Consumer Protection Act of 2019, governs consumer rights violations, unfair trade practices, and false and misleading advertisements in order to secure public and consumer protection while enforcing consumer rights. Lack of focus on broader digital dark patterns, particularly those seen in e-commerce and online platforms. No direct mention of online behavioral manipulation.	Although India's legal system addresses deceptive advertising, it is unable to fully combat digital dark patterns. By encouraging algorithmic transparency, strengthening e-commerce platform rules, and making sure digital platforms are held responsible for their actions, consumer protection can be improved.
Bangladesh	Deceptive Pattern Prevalence and User Perception: An Analysis of Bangladeshi E-Commerce Websites, 2024 [24].	According to the report, 18.3% of Bangladeshi e-commerce websites use dark patterns, and customers with greater technological expertise are more conscious of and wary of these deceptive tactics. Nevertheless, only a small number of studies on dark patterns have been carried out outside of Bangladesh and Western nations, and the research that has been presented has not thoroughly examined the psychological effects of these behaviors across many cultural backgrounds.	There is still a long way to go in terms of more efficient regulatory procedures, even though the study did point out several concerning patterns in Bangladeshi e-commerce. While governments should be in charge of putting up precise, practical legislation that would better safeguard the interests of digital customers, future research may also examine dark trends in financial services and mobile apps.
Germany	Understanding Dark Patterns in Home IoT Devices, 2023 [25].	The present study has revealed that dark patterns occur in several IoT devices, although a proportionally much higher number of these are found in the class of always on devices, including microphones and webcams. Devices from companies like Google and Amazon more frequently showed these practices than others. Still, this research is limited by its small sample size and by the brief interaction period spent with the devices, limiting the ability to accurately estimate the prevalence of dark patterns across IoT devices. Also, longitudinal effects on user behavior, privacy, and trust were not considered. More analysis with broader device coverage is required.	Although it yields valuable information about dark patterns within IoT devices, the small sample size limits generalizability of findings. Future studies should look for long-term effects, and policymakers should work to increase the transparency of IoT devices and extend mechanisms of user control.

V. CASE STUDY ANALYSIS

Case 1. Amazon was the subject of an FTC complaint in 2023. The major complaint against Amazon is that it forced users to become members of Amazon Prime without their consent while they were checking out. The design of this case scenario has identified various dark patterns that interfere with clear thinking and influence users' behavior. For example, to encourage users to become members of Amazon Prime, Amazon employed dishonest language, enticing hints, and intentionally confusing checkouts. Once users had become members, they were pressured to stay as members using confirm shaming and scare tactics, and they were discouraged from leaving Amazon Prime using a confusing and difficult cancellation process. All these activities are harmful to users' satisfaction and trust, and they are against ethical design principles; therefore, it is suggested that more emphasis should be placed on adding value and gaining users' trust than on using dishonest practices to make quick profits [26]. Hence, based on the above analysis of the case scenario, it is suggested that while developing digital products with integrity, more emphasis should be placed on adding value and gaining users' trust than on using dishonest practices to make quick profits. Invest in clear, open, and honest design that respects users' judgments and provides them with the necessary information, rather than deceiving them with false information. Make sure that important information, including terms and conditions, is easily visible and accessible. Avoid the typical mistake of burying important information in obscure places or using unreadable typefaces. Prioritizing ethical design principles and openly disclosing all expenses including membership fees will help you create a happy user base and long-term profitability.

Case 2. Fortnite and Epic Games settled with the FTC for $520 million in 2022 [27,28]. Of this sum, $275 million was fined for violating the Children's Online Privacy Protection Rule, and the balance of $245 million was set aside to compensate customers for the usage of dark patterns by the corporation. Regarding COPPA, Fortnite made a lot of mistakes. Initially, they obtained personal data from children under the age of thirteen without obtaining parental approval [29]. Additionally, they set up text and voice chat for every user automatically. Additionally, they retained the credit cards of users that is, the parents on file. Therefore, there was no need for a confirmation step when children excitedly purchased V-bucks in the game, such as asking for their ZIP code or the security number on the back of the card. Furthermore, they kept track of parents' credit card information, enabling children to buy virtual currency in the online game without having to complete an additional verification process like entering their card security code.

VI. STEPS AGAINST DARK PATTERNS EFFECTIVE HANDLING IN INDIA

6.1 Regulatory Framework and Guideline

India has recognized and addressed these patterns. False Urgency, Confirm Shaming, Forced Action, Bait and Switch, Drip Pricing, Basket Sneaking, Trick Questions, SaaS Billing, Rogue Malware, Disguised Advertisements, Nagging, Subscription Traps, and Interface Interference are among the 13 recognized categories of dark patterns. Regulations designed to stop these misleading tactics have come under fire for being unnecessary, unduly wide, and having unexpected effects on the digital environment. Although the goal of these guidelines is to safeguard consumers from harmful practices such rogue virus and deceptive marketing, some contend that the Information Technology Act of 2000 [30] and other current legislation are frequently more appropriate for addressing these kinds of issues. International frameworks such as the California Consumer Privacy Act (CCPA) serve as inspiration for the standards, which emphasize the importance of ethical design, user control, and openness in digital platforms. Nonetheless, it is imperative that regulations be explicit and well balanced in order to protect consumer rights without impeding lawful corporate operations.

6.2 Prevention of Misleading Advertisements guideline of CCPA

Prevention of Misleading Advertisements guideline of CCPA: On June 9, 2022, the CCPA released new rules with the goal of strengthening consumer protection against false, unrealistic, irrational, and misleading statements in marketing. These rules are supported by Section 18 of the Consumer Protection Act (CPA), 2019, which protects consumer rights as outlined in Section 2(9) of the CPA 2019 and includes the rights to information, choice, and protection from deceptive goods and services. All media, including print, radio, television, and social media, are subject to the standards. They are an addition to the rules already in place under other laws, like the Cable Television Networks (Regulation) Act of 1995 (7 of 1995) and the Press Council Act of 1978 (37 of 1978) [31].

6.3 Public Awareness Campaigns

The Department of Consumer Affairs, Government of India, announced the "Dark Patterns Buster Hackathon 2023" in association with IIT-BHU. The goal of the hackathon is to create cutting edge tools that can identify dark patterns frequently seen on e-commerce platforms, such as mobile applications, plugins, add-ons, and browser extensions. It is recommended that participants concentrate on aspects such as security of privacy, cross browser interoperability, intuitive user interfaces, and accuracy of pattern identification [32].

6.4 Enhanced Penalties and Enforcement

Under the Consumer Protection Act of 2019, the CCPA in India is principally responsible for directing stricter penalties and enforcement actions related to dark patterns. There are serious consequences for breaking the rules governing dark patterns. In particular, platforms that participate in deceptive advertising or dark pattern activities may be subject to fines of up to ₹10 lakhs, with the potential for fines of up to ₹50 lakhs for recurrent infractions. In order to safeguard consumer rights, the CCPA rules place a strong emphasis on the obligation of platforms and advertisers to maintain fairness and transparency in their digital interfaces.

Under the Consumer Protection Act, dark patterns which include actions such as forced action, rogue malware, false urgency, and confirm shaming are considered unfair business practices and infringement of consumers rights. The standards are meant to prevent companies from incorporating deceptive design techniques into their user interfaces, guaranteeing moral user experiences that put the autonomy and choice of the customer first.

The proposed approach for formation of legal provisions to detect and safeguard the user privacy is given in the Figure 1. There is an immediate need to work on the varied GUI from different categories, Online entertainment platforms, web browsers, mobile applications to find out the hidden dark patterns based on their usage and context. Once identified the legal considerations to make them ethical by removing the deceptive text, changing the navigation path, editing the permissions given by default and revisions in access control etc. are possible with the policies, regulations and effective guidelines

Figure 1. Proposed approach for data privacy protection

6.5 Proposed Dark Pattern Detector Framework

The proposed framework presented in Figure 2, represents an automated dark pattern detection system. It may use a web crawler to collect webpage URLs. An algorithm based on the text string mostly used by a certain type of dark pattern maybe detected using regular expressions. By storing these dark patterns, the repository can be created to guide and suggest the e-commerce as well

as other websites to change their GUI and remove the dark patterns. This will help to protect the end user privacy and also to stop the financial scams performed by these websites. Guideline to adhere the practices are required and the proposed framework maybe utilized to develop solution for it.

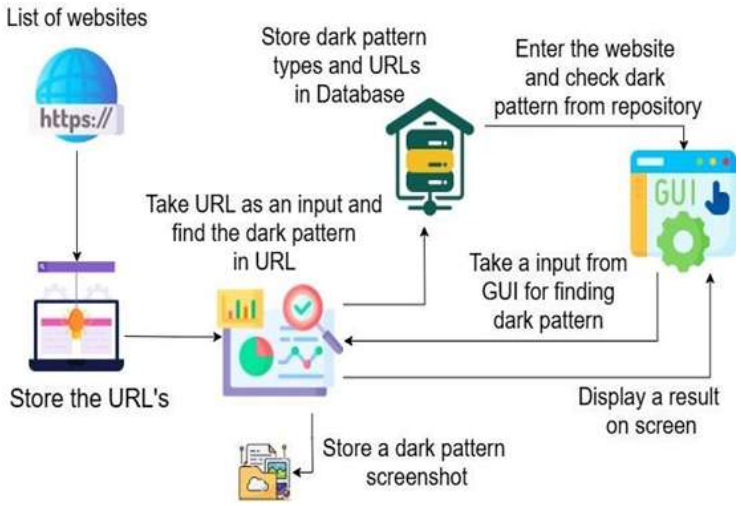

Figure 2. Dark pattern Detector framework

VIII. CONCLUSION

In order to provide a more comprehensive understanding of this widespread problem, the study looks at how dark patterns manifest in digital interfaces worldwide from the perspectives of multiple countries and legal systems. This paper aims to emphasize a growing concern in the global arena, that dark patterns are not beneficial to user experiences and consumer rights. It is done by comparing various research and recommendations of laws in the United States, European Union, South Korea, India, Canada, and Bangladesh. Some of these countries are beginning to enact laws or policies to prevent these kinds of dishonest practices, although it is done in various ways, and most of the time, it is not effective. The use of coercion, the spread of misinformation, and dishonest user interface design are some of the common underlying factors of dark patterns, despite their differences in definition and law. Conclusion of this research is that, especially in online business, consumers who are tech-savvy are becoming aware and suspicious of these practices. It also emphasizes how important it is to abide by changing laws and to gain the trust of consumers with ethical design principles that value user autonomy.

IX. FUTURE SCOPE

The future of research in dark patterns is a promising area with a number of opportunities for furthering our understanding of dark patterns and mitigation strategies. In order to have a truly worldwide understanding of dark patterns, future research should be focused on furthering cross-cultural studies and conducting in-depth studies of the long-term psychological effects of dark patterns. In terms of technology, there is a great deal of room for furthering the development of AI-based technologies that are capable of automatically identifying dark patterns. International cooperation is also necessary in order to create a uniform system of regulations and effective regulations. The future of dark patterns should also involve studying the effects of dark patterns on society and the economy, dark patterns in virtual and augmented reality technologies, and dark patterns in digital accessibility. This furthering of our understanding of dark patterns will continue to build upon our previous understanding of dark patterns and inform a more ethical digital design practice.

In order to formulate uniform laws with effective enforcement provisions, there also exists the need for more cooperation on the international front. To understand the impact of the social and economic implications of dark patterns, how they are being integrated into the newer forms of technology such as virtual and augmented reality, and how they will influence digital accessibility, further research has to be done. Such advancements in the field of research will enable a better understanding of the concept of dark patterns and lead to more effective interventions in the field of user-centered and ethical digital design.

REFERENCES

[1] Leiser, M. R. 2022. Dark patterns: The case for regulatory pluralism between the European Union's consumer and data protection regimes. In Research Handbook on EU Data Protection Law. Edward Elgar Publishing, pp. 240–269.
[2] King, J. and Stephan, A. 2021. Regulating privacy dark patterns in practice: Drawing inspiration from the California Privacy Rights Act. Georgetown Law Technology Review, 5(2): 250–276.
[3] Wilson, L. 2023. Is there a light at the end of the dark-pattern tunnel? George Washington Law Review, 91: 1048–1065.
[4] Pasanen, V. 2022. Regulating dark patterns through the GDPR and DSA: The potential for a legal loophole? Master's Thesis.
[5] Ruohonen, J. and Hjerppe, K. 2022. The GDPR enforcement fines at a glance. Information Systems, 106: 101876.
[6] Leiser, M. and Santos, C. 2023. Dark patterns, enforcement, and the emerging digital design acquis: Manipulation beneath the interface.
[7] Federal Trade Commission. 2022. Bringing dark patterns to light. FTC Report, September 2022.
[8] Korean Fair-Trade Commission. 2023. Developing regulations on dark patterns.
[9] Central Consumer Protection Authority, Government of India. 2023. Guidelines for prevention and regulation of dark patterns, 30 November 2023.
[10] Asia Internet Coalition. 2023. Guidelines and suggestions on dark patterns for India, October 2023.
[11] Tran, V. H., Mehrotra, A., Sharma, R., Chetty, M., Feamster, N., Frankenreiter, J. and Strahilevitz, L. 2024. Dark patterns in

the opt-out process and compliance with the California Consumer Privacy Act (CCPA). arXiv preprint, arXiv:2409.09222.
[12] Carter, M. 2024. The optimal opt-in option. Columbia Law Review, 124(2): 431–458.
[13] O'Connor, S., Nurwono, R., Siebel, A. and Birrell, E. 2021. (Un)clear and (in)conspicuous: The right to opt-out of sale under CCPA. In Proceedings of the Workshop on Privacy in the Electronic Society, pp. 59–72.
[14] California Privacy Protection Agency. 2023. Final regulations text on CCPA penalties.
[15] Sun, C., Jacobs, E., Lehmann, D., Crouse, A. and Shastri, S. 2023. GDPRxiv: Establishing the state of the art in GDPR enforcement. Proceedings on Privacy Enhancing Technologies.
[16] Federal Trade Commission. 2023. Penalty offenses.
[17] Mamidwar, A. and Bhutkar, G. 2024. An overview of guidelines on dark patterns.
[18] Mathur, A., Acar, G., Friedman, M. J., Lucherini, E., Mayer, J., Chetty, M. and Narayanan, A. 2019. Dark patterns at scale: Findings from a crawl of 11K shopping websites. Proceedings of the ACM on Human-Computer Interaction, 3(CSCW): 1–32.
[19] Nouwens, M., Liccardi, I., Veale, M., Karger, D. and Kagal, L. 2020. Dark patterns after the GDPR: Scraping consent pop-ups and demonstrating their influence. In Proceedings of the CHI Conference on Human Factors in Computing Systems, pp. 1–13.
[20] Bielova, N., Litvine, L., Nguyen, A., Chammat, M., Toubiana, V. and Hary, E. 2024. The effect of design patterns on cookie consent decisions. In Proceedings of the USENIX Security Symposium, pp. 2813–2830.
[21] Canadian Bar Association. 2022. A case for regulatory reform in Canada.
[22] Gaulton, M., Kelly, D. and Burkell, J. 2024. Approaches to regulating privacy dark patterns.
[23] Government of India. 2022. Guidelines for prevention of misleading advertisements.
[24] Sazid, Y. and Sakib, K. 2024. Prevalence and user perception of dark patterns: A case study on e-commerce websites of Bangladesh. In Proceedings of ENASE, pp. 238–249.
[25] Kowalczyk, M., Gunawan, J. T., Choffnes, D., Dubois, D. J., Hartzog, W. and Wilson, C. 2023. Understanding dark patterns in home IoT devices. In Proceedings of the CHI Conference on Human Factors in Computing Systems, pp. 1–27.
[26] Federal Trade Commission. 2023. FTC action against Amazon Prime enrollment scheme.
[27] Parra, A. 2024. Coping with COPPA: Exploring alternatives to the Children's Online Privacy Protection Act. Indiana Journal of Law and Social Equality, 12(2).
[28] Rosenbloom, M. 2023. Clearing the darkened air: Regulating dark patterns as air pollution. Minnesota Journal of Law, Science & Technology, 25: 139.
[29] Steinberg, S. 2024. The myth of children's online privacy protection. SMU Law Review.
[30] Rajya Sabha Secretariat. 2023. Action against misleading advertisements.
[31] Palit, M. 2024. Protecting online consumers: A deep dive into dark pattern regulations in India. International Journal of Creative Research Thoughts (IJCRT), 12(2): c238–c243.
[32] Press Information Bureau, Government of India. 2023. Centre launches 'Dark Patterns Buster Hackathon 2023', 5 October 2023.