Analysis of Dark Patterns and Law for Use of Information in Digital World

Amit Kumar Jha[1*], Dr. Saket Sharma[2]

[1]PhD Research Scholar, School of Law, Galgotias University,
Plot No.2, Sector 17-A Yamuna Expressway, Greater Noida, Gautam Buddh Nagar, Uttar Pradesh 203201, India
ORC Id: 01-02-01-02, Email Id: amit.22gsol13010013 _phd22@galgotiasuniversity.edu.in, amitjha1976@gmail.com

[2]Designation: Associate Professor Galgotias University PhD Research Scholar, School of Law, Galgotias University, Plot No.2, Sector 17-A Yamuna Expressway, Greater Noida, Gautam Buddh Nagar, Uttar Pradesh 203201, India ORC Id: 01-02-01-02, Email Id: amit.22gsol13010013_phd22@galgotiasuniversity.edu.in, amitjha1976@gmail.com

HOW TO CITE:
Amit Kumar Jha , Saket Sharma (2026). Analysis of Dark Patterns and Law for Use of Information in Digital World. International Journal of Special Education, 41(17s), 949-965

COPYRIGHT STATEMENT:
Copyright: © 2026 Authors. Open access publication underthe terms and conditions of the Creative CommonsAttribution (CC BY) license (http://creativecommons.org/licenses/by/4.0/).

ABSTRACT:
Dark patterns refer to any practice or encoding of a design that leads users to make decisions that they wouldn't have otherwise made freely and knowingly. They are often found on websites, mobile apps, eCommerce sites, subscription services, ads, cookie banners and privacy interfaces. The aim of this paper is to analyse and discuss the impact of dark patterns on consumer autonomy, informed consent, privacy and use of personal data in the digital world. The study is doctrinal and analytical in nature, utilising relevant statutes, regulatory guidelines, policy reports and other literature. It examines the typology of dark patterns and their effect on information use, and the effectiveness of legal remedies in these different jurisdictions, including India. The study concludes that not only are dark patterns an unethical design strategy but that they are an important legal tool of digital manipulation which can result in consumer, privacy, contractual, and autonomy related harms. It calls for the interface design to be transparent, meaningful consent, withdrawal options to be easy, enforcing effectively and platform accountability.

Keywords: Consumer Protection; Informed Consent; Data Privacy; Deceptive Design; Online Manipulation; Information Use; Unfair Trade Practices; Platform Accountability; Digital Governance.

1. Introduction

The swift development of the digital platforms has changed the way people communicate, buy products and services, obtain information and make choices online. Across websites, mobile apps, ecommerce, subscription services, social media and digital payment systems, users are making more decisions than ever before about making purchases, privacy settings, cookies and their personal data, ads, and consent.

While the purpose of the design of digital interfaces is to facilitate the interaction of the user on the internet, it can also be used to shape or even manipulate user behaviour. This is referred to as dark patterns. They guide users towards options they might not have chosen voluntarily or without understanding, such as creating false pressure, withholding important information, charging users extra amounts, making it harder to opt-out or to make privacy-protective choices.

Dark patterns are an outgrowth of user experience design. Dark patterns are currently defined as a design ethics problem where users' goals and aspirations are substituted with business or manipulative goals (Gray et al., 2018). Platforms know how to appeal to users' sense of urgency, defaults, salience, emotion and difficulty to navigate. Such knowledge can be used to gain a commercial edge at the expense of the user's autonomy, making the design legally and ethically questionable.

Dark patterns are particularly prevalent in online marketplace platforms that are trying to maximize their sales, subscriptions, engagement, data collection, or advertising revenue. A study on a large number of shop websites concluded that the use of dark patterns is to encourage consumers to buy or to provide more information than they would otherwise give (Mathur et al., 2019). It demonstrates that dark patterns are not in isolation, but are integrated practices in the design of platforms.

Dark patterns are legally relevant as they impact on consumer autonomy as well as informed consent, consumer privacy, transparency and fair digital choice. Click "accept," "continue," "subscribe," or "buy now" may appear to be a formal act, but if the interface is designed to confuse, pressure, obstruct and/or mislead, its validity may be questionable. The worry is particularly strong if platforms are gathering personal data via cookies, tracking, notifications, identity info and/or regular registrations.

These risks have been more evident to regulators. For the Federal Trade Commission, dark patterns have been the hallmark of deceptive or unfair practices by companies that force customers to make a purchase or give up data via design tricks (Federal Trade Commission, 2022). The issue is especially relevant in India where the e-commerce sector and other digital payments and applications are rapidly expanding and data informing and shaping business models is becoming increasingly common. This study aims to answer the question of if there is already a consumer protection framework, privacy and digital governance, that is adequate to control the deceptive design practices.

Dark patterns are only considered in the context of digital platforms, such as websites, mobile applications, e-commerce services, subscription services, online advertisements, cookie consent banners, privacy interfaces and app-based services. It centres on dark patterns which impact consumer choice, informed consent, privacy, personal information and online transactions. Does not analyze offline unfair trade practices, unless they are relevant in understanding online manipulation.

The study makes a contribution to the field of law by looking at dark patterns as a consumer protection, data protection, advertising and a digital governance issue. It is relevant in India's context as India has identified certain dark patterns in its regulations, and enforcement and platform accountability are still emerging issues.

The research method in this study is doctrinal and analytical studies with legal. It is conceptual and based on legal materials, regulatory documents, policy reports and academic literature. The doctrinal aspect covers statutory requirements, guidance from government and regulator, reporting requirements and law applicable to dark patterns . The analytical part analyzes impact of dark patterns on consumer autonomy, informed consent, privacy and information use. The study also reflects on existing dark-pattern scholarship both to pinpoint main themes, definitions, classifications and legal issues (Isola and Esposito, 2025; Gray et al., 2023).

Primary and Secondary sources are used. Primary sources are consumer protection legislation, consumer protection guidelines, data protection principles and regulatory materials. Secondary sources are the journal articles, conference papers, legal commentaries, research reports and policy documents. By using a comparative approach, Indian, European Union and United States responses to dark patterns are referred to.

The present study aims to examine dark patterns as a legal and regulatory concern in the digital

environment. The specific objectives of the study are:

- To understand the concept, nature, and major forms of dark patterns used in digital platforms.
- To analyse how dark patterns affect consumer autonomy, informed consent, privacy, and use of personal information.
- To examine the legal framework relating to dark patterns under consumer protection, data protection, and digital governance laws.
- To suggest legal, regulatory, and policy measures for preventing deceptive and manipulative digital design practices.

2. Literature Review

Dark patterns literature has spanned law, human-computer interaction, data protection and consumer protection, behavioural economics, and digital governance and information systems. Dark patterns have already been studied and found not to be a technical defect or poor choice of interface. They are digital practices that attempt to influence the decisions you make online through manipulating the information, consent, purchase options, privacy options and cancellation procedures. For the purpose of this study the literature is broken down into three aspects of themes: legal and regulatory scholarship, privacy and consent-based scholarship, and consumer vulnerability or digital abuse scholarship.

2.1 Legal and Regulatory Literature

As demonstrated in the legal literature, there is an overlap of issues with consumer protection and data protection law with regard to dark patterns. A key contribution is that dark patterns violate the necessary legal principles of valid consent, fairness, transparency, privacy-by-design and users' control over their personal data. Consumer choice and data protection rights could both be impacted by the same design practice so there may be a need for a single legal regime to cover both. Thus, a pluralistic approach, involving both consumer protection and data protection law is necessary (Leiser, 2022).

A second genre of literature is on the enforcement and regulatory designs of dark patterns. It asserts that deceptive design doesn't always have to take place at the interface level, but can also be a part of the architecture of the digital system. Therefore, regulators need to consider how a screen displays the information, how things are set by default, how data flows, friction, and the order in which users interact (Leiser and Santos, 2023).

The literature also associates dark pattern regulation with consumer's autonomy. Dark patterns would often lie in a grey area between persuasion and manipulation, which is lawful. They become an issue when they take advantage of behavioural biases, hide material information, put in needless obstacles, or obstruct user ability to make an informed decision (Brenncke, 2024). This contradicts the view held by the law that disclosure is enough, as information can be available in an explicit way while the interface is structured to conceal, inundate, twist or emotionally manipulate these data.

2.2 Privacy, Consent, and Harms Literature

Much of the literature is devoted to dark patterns and privacy/consent. Dark patterns are specifically relevant as they often occur when users are prompted to accept cookies, provide personal information, allow tracking, sign up for accounts, enable notifications, agree to terms, or maintain their subscription. Such interactions have a direct impact on the collection and processing of personal data.

The literature on privacy harms outlines that dark patterns can induce material harms (e.g. through unwanted payments, recurring charges) and non-material harms (e.g. privacy violation, cognitive overload, emotional stress, loss of control, diminished trust in online services). This demonstrates the need not to consider dark patterns solely from a monetary perspective, but also one of law and social harm from the consent manipulation and the illegal or inappropriate use of personal data (Gunawan et al., 2022).

Research about cookie consent requests reveals that cookie consent interfaces are a prime target

for dark patterns. Cookie banners can incentivize users to make privacy-exposing decisions, by making them more visible and salient than rejecting decisions, which might be hidden, delayed, or otherwise made more difficult. A concept of "bright patterns" is also helpful as it demonstrates that design can help or hinder lawful consent (Graßl et al., 2025).

Consent-banner scholarship also holds that consent needs to be evaluated as an interaction, rather than a single click. Use of options, steps needed to refuse consent, language of option, defaults and social environment all impact the meaningfulness of consent (Gray et al., 2021). More recent literature also makes it clear that the negative effects of dark-pattern can overlap in data protection, consumer protection and competition law and this makes it difficult to classify them in the legal world and to enforce (Santos et al., 2025).

On balance, it is possible to conclude that a user's agreement cannot be regarded as truly free and informed if the interface puts in place obstacles to rejection, causes the user to get confused, induce fatigue, or exerts pressure to accept.

2.3 Consumer Vulnerability and Digital Abuse Literature

There is literature in the field of consumer vulnerability which demonstrates that dark patterns impact not just traditionally vulnerable consumers. In the past, the legal analysis has been directed at vulnerable groups like children, elderly people, people with disabilities or low income consumers, but recently studies have indicated that all digital consumers could be in a vulnerable situation in a manipulative digital choice environment. Dark patterns in Web Design take advantage of some of the common habits and behaviors of users such as the default behavior, urgency, FOMO, trust cues and decision fatigue (Zac et al., 2025).

The empirical research provides evidence of the notion that dark patterns can impact users of all age groups, which contradicts the idea that they only impact a certain subset of users. Meanwhile, others could be at higher risk for various reasons such as age, digital literacy, economics, device type, language abilities, disability or urgency of need. Vulnerability in the digital world is thus multi-faceted and can be caused, not only by personal factors, but also by the design of the services, the situation in which the transactions are entered, the dependence on services and the complexity of the privacy interfaces (Rossi et al., 2024).

To some, scholarships that are presented in this way constitute digital abuse as they take advantage of the power disparity between platforms and users. Platforms dictate the course of actions; what users see and don't see, the sequence in which they see the information, and the pathways through which their actions can be carried out; users are often short of time, information and bargaining power (Boris et al., 2024). Dark patterns also tie in to engagement, subscription, advertising, retention and data collection revenue models for platforms from a business and information systems point of view. This is why the practice is still carried out, even though it is illegal and unethical (Kollmer and Eckhardt, 2023).

Combined, the vulnerability and digital abuse literature reveals that dark patterns are based on influencing behaviour, controlling platforms, maintaining information asymmetry, and commercial incentives. Focusing on the regulation of single instances of misleading decision making will, therefore, not suffice, but rather the overall digital space in which users are (repeatedly) confronted with deception-induced options must be regulated.

2.4 Research Gap

There are ample resources to learn about dark patterns from a design perspective, behavioural perspective, privacy perspective, consumer protection perspective and regulatory perspective. But there is a disconnect in all these strands that have not yet been synthesized into a specific legal study of dark patterns, consumer autonomy and information use, and the Indian regulatory response. Much of the literature is EU and U.S. focused. While certain dark patterns have been identified in law through the

regulations, there is a need to analyse the relation of those categories with privacy, consent, personal information, unfair trade practices and digital governance. The current study tries to fill this void and explore dark patterns as a multifaceted phenomenon of consumer protection, information use, privacy and legal accountability in the digital sphere. The reviewed literature is summarised in Table 1 according to its focus area, methodology, contribution, and relevance to the present study.

Table 1: Summary of Literature Review

Reference	Focus Area	Methodology/Approach	Key Contribution	Relevance to Present Study
Leiser (2022)	Consumer protection and data protection regulation	Doctrinal legal analysis	Explains the need for regulatory pluralism between consumer and data protection regimes	Supports the legal framework discussion
Leiser and Santos (2023)	Enforcement and digital design regulation	Legal and policy analysis	Shows that manipulation may exist both at interface level and beneath the interface	Supports platform accountability analysis
Brenncke (2024)	EU regulation and autonomy	Doctrinal legal analysis	Places consumer autonomy at the centre of dark-pattern regulation	Supports analysis of autonomy and manipulation
Gunawan et al. (2022)	Privacy harms and redress	Literature review and legal analysis	Identifies material and non-material harms caused by dark patterns	Supports privacy, harm, and redress discussion
Graßl et al. (2025)	Cookie consent requests	Privacy design and experimental analysis	Shows how consent interfaces influence privacy decisions	Supports the information-use section
Gray et al. (2021)	Consent banners	Interaction criticism and legal analysis	Connects interface design with legal consent requirements	Supports analysis of consent validity
Santos et al. (2025)	Harms under EU law	Legal analysis	Examines dark-pattern harms under data protection, consumer, and competition laws	Supports comparative legal analysis
Zac et al. (2025)	Consumer vulnerability	Empirical behavioural study	Shows that dark patterns may affect users across different groups	Supports vulnerability analysis
Rossi et al. (2024)	Digital vulnerability	Transdisciplinary analysis	Explains vulnerability as multi-dimensional in digital environments	Supports consumer protection argument

Boris et al. (2024)	Digital abuse	Legal and social analysis	Treats dark patterns as manipulative digital abuse	Supports broader governance discussion
Kollmer and Eckhardt (2023)	Business and information systems	Conceptual/business analysis	Explains dark patterns in platform and commercial contexts	Supports commercial motivation analysis

3. Dark Patterns, Information Use and Legal Framework

Dark patterns are a complex design, consumer behaviour, information use and law issue. It's not just about incorrect buttons or confusing layouts, it's about a digital choice architecture that shapes how users make choices. In this section, the conceptual understanding and classification of dark patterns, their connection with information use and the legal regulation are explored.

3.1 Conceptual Framework of Dark Patterns

Dark patterns can be defined as deceptive, manipulative and/or coercive design elements that impair the user's ability to make self-served and informed decisions to achieve an end in a digital system. They navigate by using the elements of the digital interface such as buttons, colours, defaults, pop-up windows, consent banners, hidden links, confusing labels, repetitive prompts and complicated navigation paths. Their purpose is to lead the user towards a decision desired by the site and it does not necessarily benefit the user.

Dark patterns are based on a core idea that the digital design isn't 'neutral'. A platform can offer two or more alternatives to the user, but the design might make one easier or faster, more obvious or more appealing to the user than the other. For instance, an "Accept All" button can be made to stand out in a bright colour and the "Reject" can be placed at a number of steps. While it may be easy to sign up for a subscription, it may be hard to cancel it. At the time it seems like a cost-effective product, and only the extra fees are made known at the very end of the payment process. These illustrations demonstrate that as well as the content of information, the structure in which information and choices are given, are also harmful.

It's helpful to think of a conceptual layering when considering dark patterns. The design layer is the first layer in which the placement, colour, font size, checkboxes, banners and other interface elements like buttons, icons, defaults etc. are used. The second layer is behavioural; "urge customers to act now, let customers know that things are running out, instill fear etc.". The user impact level is the third level, where the user might make an unwanted purchase, click on tracking, renew a subscription, provide personal information or not assert a right. The fourth is the legal layer, which could involve an issue of unfair trade practice, invalid consent, misleading advertisement, privacy violation or data misuse.

Recent scholarship has sought to create a common set of definitions and categories between design, law, regulation and technology to make possible an ontology of dark patterns. This is significant because there is a difference in terminology across disciplines for practices that are similar. So, what is interface interference to the designer, may be considered a misleading presentation by a consumer lawyer, and a violation of consent by a data protection regulator. These perspectives can be linked together in a common conceptual framework, which will facilitate legal analysis (Gray et al., 2024).

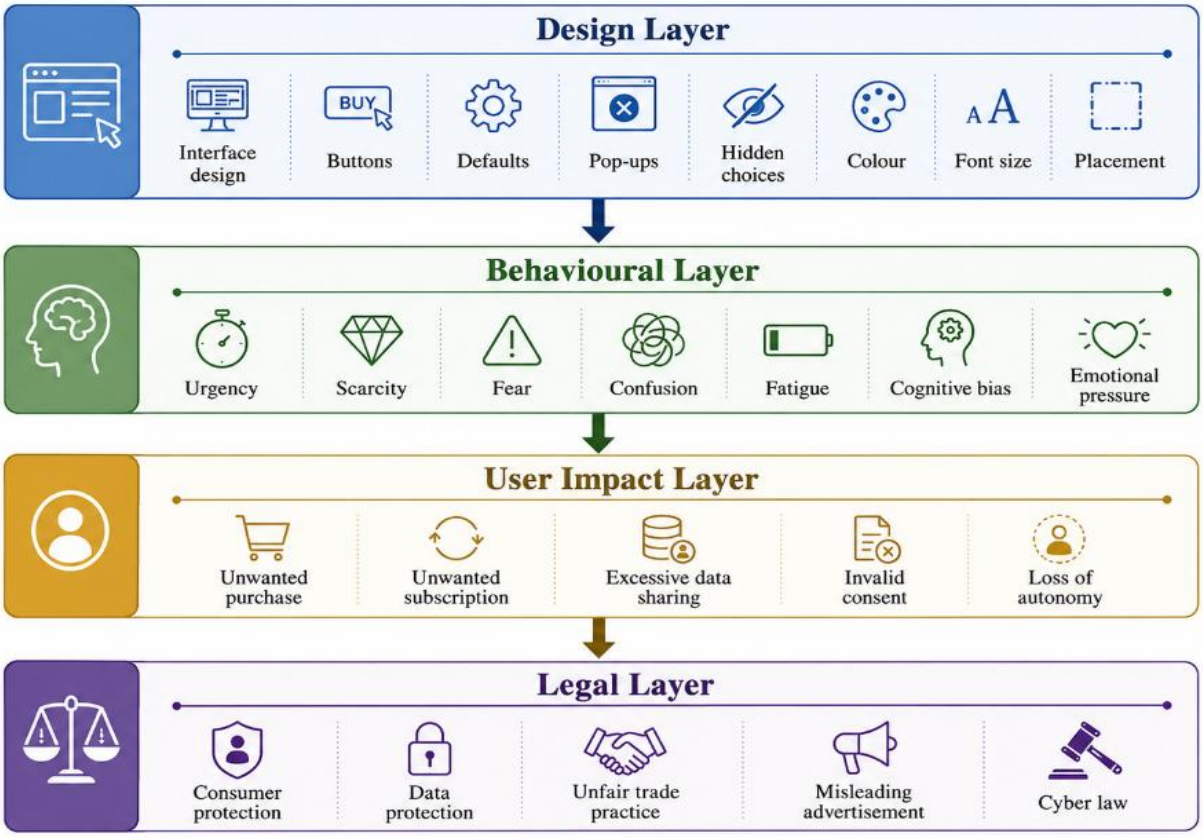

Figure 1: Conceptual Framework of Dark Patterns

This figure 1 schema depicts the dark patterns as not just design issues. They form an interface design that stems to legal harm. Design layer influences the behavioural layer, behavioural layer influences the user's decision, and the user's decision may lead to legal consequences. Hence, the control of dark patterns must include looking at the interface design, as well as the impact on the user's autonomy, consent and control of information.

3.2 Classification of Dark Patterns

Dark patterns come with a classification, which matters as law enforcement needs a list of categories of harm in order to regulate. The Central Consumer Protection Authority (CCPA), as part of the Indian framework, has issued Guidelines for Prevention and Regulation of Dark Patterns, 2023, which list thirteen dark patterns. These categories offer a systematic way for analysing deceptive design practices in digital platforms (Central Consumer Protection Authority, 2023).

There are thirteen categories which include a broad spectrum of manipulative practices. Some dark patterns are based on pressure - false urgency and confirm shaming. Some use tactics to conceal or raise costs, like basket sneaking and drip pricing. Some interfere with user freedom, for example subscription traps, forced action and interference with the user interface. Others deceive their users by misrepresenting the product in some way, like bait and switch, disguised advertisement, trick questions, SaaS billing, nagging and rogue malware Table 2 presents the major categories of dark patterns recognised under the Indian Guidelines and their related legal concerns..

Table 2: Classification of Dark Patterns under Indian Guidelines

Dark Pattern	Meaning	Example	Legal Concern
False urgency	Creating a false sense of limited time, scarcity, or high demand	"Only 2 rooms left" or "Sale ends in 10 minutes" when not true	Misleading representation and pressure-based consumer manipulation
Basket sneaking	Adding extra goods, services, donations, or charges to the cart without clear consent	Automatically adding travel insurance during flight booking	Unfair trade practice and absence of informed consent
Confirm shaming	Using guilt, fear, shame, or ridicule to influence user choice	"No, I do not care about my safety" when rejecting insurance	Emotional manipulation and interference with free choice
Forced action	Requiring the user to perform an unrelated or unnecessary act to access a service	Forcing newsletter subscription or unnecessary personal data sharing	Coerced consent and excessive data collection
Subscription trap	Making subscription cancellation impossible, hidden, or unnecessarily difficult	Easy sign-up but multi-step hidden cancellation	Consumer lock-in and unfair billing practice
Interface interference	Manipulating visual design to hide or weaken important choices	Bright "Accept" button and faint "Reject" button	Misleading interface and invalid consent
Bait and switch	Promising one result but delivering another	Product shown as available, then replaced by a costlier option	Deceptive advertisement and unfair commercial practice
Drip pricing	Revealing extra charges gradually or at the final stage	Extra platform fee added only at checkout	Price deception and lack of transparency
Disguised advertisement	Presenting advertisement as genuine content, news, or user material	Sponsored post appearing as independent review	Misleading advertisement and lack of disclosure
Nagging	Repeatedly interrupting or pressuring users to take an action	Continuous pop-ups to enable notifications or download an app	User harassment and manipulative pressure
Trick question	Using confusing wording or double negatives to mislead the user	"Do you wish to opt out of not receiving updates?"	Confused consent and unfair choice architecture
SaaS billing	Using deceptive recurring billing or silent auto-renewal practices	Free trial converted into paid subscription without clear notice	Unfair billing and lack of transparency
Rogue malware	Using fake warnings or scareware to mislead users into harmful actions	Fake virus alert demanding payment for removal	Cyber fraud, security risk, and digital deception

As this classification reveals, dark patterns are not a one-size-fits-all type of misconduct. They can do this via pressure, hidden costs, obstruction, misrepresentation, interfering with privacy, billing fraud or cyber deception. The classification is of legal value because it links digital design practices to easily identifiable legal issues of unfair trade practices, misleading advertisements, no consent, privacy violation, and cyber harm.

3.3 Dark Patterns and Use of Information in the Digital World

Being in the digital world involves information use, which is related to consent, privacy and user autonomy. The personalisation, profiling,

engagement, advertising, payment, subscriptions and service delivery are all dependent on personal information, which digital platforms rely on. Dark patterns can be an issue when they are used to acquire access to such information at a time when there is little or no control by the user.

Dark patterns can impact user information by coercing the user to accept cookies or tracking, prompting the user to reveal phone number information, ID information, location information, contact information or access to their social media and forcing the user to choose privacy settings that are challenged to find or change. An interface in such cases could make it more convenient to make privacy-invasive options than privacy-protective options.

Another big problem is what's known as consent fatigue. Pop up, banners, notices, forms and permission requests, are frequently repeated. With time they may be tempted to select the quickest one as opposed to the most educated selection. Platforms can take advantage of this fatigue by presenting making those acceptances more salient and easier than the rejections. So, the user's apparent consent can be interpreted as not truly being a free and informed choice.

Dark patterns also help to build information asymmetry: platforms typically know exactly how users react to prompts, timing and appearance of the buttons while users don't necessarily know how the interface affects them. Platforms are able to gather more data, keep users, drive higher sales or obtain repeat payments, due to this imbalance. Dark patterns, therefore, become a consumer protection issue, as well as a privacy issue.

Dark pattern and information use is particularly evident in cookie banners, privacy dashboards, app permissions, subscription interfaces and account terminations. The more difficult, hidden or confusing such designs are to make privacy-protective choices, the less control the user has over his or her personal information.

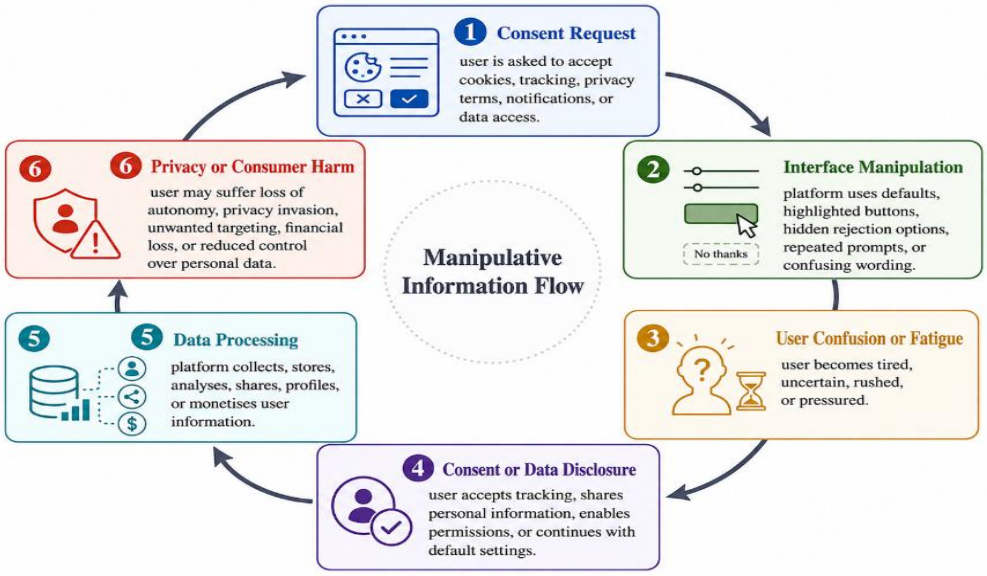

Figure 2: Dark Patterns and Information Misuse Cycle

This figure 2 cycle demonstrates how dark patterns can turn a 'consent' cycle into an information extraction cycle. The evaluation of whether the user has clicked a button should thus also take into consideration the type of design surrounding the button, which allows a meaningful and informed decision by the user.

3.4 Legal Framework

A multi-faceted response to the legal regulation of dark patterns is needed, that combines consumer protection, data protection, advertising regulation and digital governance. Dark patterns can impact purchases, subscription, consent, privacy and data use – and they're not necessarily

governed by just one type of law. All of these can be considered one practice at a time, or one practice can be considered a violation of multiple issues, such as unfair trade practice, misleading advertisement, privacy violation, or platform accountability.

Dark patterns have been primarily discussed in India under the consumer protection legislation and regulation of digital platforms. They are particularly pertinent in e-commerce, online advertising, application services and subscription services, where consumers rely on interface design to comprehend how much and what they are paying for, how to cancel and what the privacy implications are (Sharma, 2023). The Indian scholarship also points out that dark patterns are based on information asymmetry and also decrease the consumer's capability to make a free and informed choice (Chugh and Jain, 2021).

Indian legislations include the Consumer Protection Act, 2019, Consumer Protection (E-Commerce) Rules, 2020, Guidelines for Prevention and Regulation of Dark Patterns, 2023, Guidelines for Prevention of Misleading Advertisements and Endorsements, 2022, and Digital Personal Data Protection Act, 2023. These tools are applicable whenever dark patterns are used to trick users into paying hidden fees, making them feel pressured to make a purchase, deceive them about advertising, enter into unwanted subscription services, make them consent to something they wouldn't otherwise, or misuse personal data.

By contrast, the European Union (EU) has a series of overlapping regulations that deal with dark patterns, including the GDPR, Unfair Commercial Practices Directive, Digital Services Act and Digital Markets Act. The laws apply to consent and transparency, privacy settings, platform accountability and unfair digital choice architecture. Dark patterns are considered to be unfair or deceptive practices under the Federal Trade Commission Act in the United States, particularly when the hidden charges or the subscription trap occurs, the cancelling process is not clear, unwanted cart additions are performed, and privacy-choice manipulation is seen. Table 3 compares the legal treatment of dark patterns in India, the European Union, and the United States.

Table 3: Comparative Legal Framework on Dark Patterns

Jurisdiction	**Legal Instrument**	**Main Concern**	**Examples of Regulated Conduct**
India	Consumer Protection Act, 2019; Consumer Protection (E-Commerce) Rules, 2020; CCPA Guidelines for Prevention and Regulation of Dark Patterns, 2023; Digital Personal Data Protection Act, 2023	Unfair trade practices, misleading advertisements, consumer manipulation, consent, and personal information	False urgency, basket sneaking, drip pricing, disguised advertisement, forced action, subscription trap
European Union	GDPR; Unfair Commercial Practices Directive; Digital Services Act; Digital Markets Act; Data Act; AI Act	Data protection, consent, autonomy, platform accountability, unfair commercial practices, and digital choice architecture	Deceptive consent banners, manipulative privacy settings, obstruction, hidden information, unfair platform design
United States	FTC Act; FTC enforcement policy; California privacy laws including CCPA/CPRA	Unfair or deceptive acts, subscription traps, hidden charges, privacy choice manipulation, and consumer deception	Pre-checked boxes, difficult cancellation, unwanted cart additions, hidden fees, misleading interface design

Within the comparative framework, it is revealed that dark patterns are acknowledged as a legal issue in jurisdictions. But they are controlled through various legislative avenues in different jurisdictions. India has taken a certain step towards identification of dark patterns in the consumer protection guidelines. There are three ways in which the European Union deals with the issue: consumer protection, data protection, platform regulation. Unfair and deceptive practice enforcement is a critical tool that the United States uses. This relative context implies that dark patterns cannot be addressed by a piecemeal or single-law solution.

4. Analysis and Discussion

Dark patterns pose a substantial problem for the legal regulation: They are sometimes not obvious fraud or even explicit misrepresentation. In many instances they work by means of a design that may seem very simple but actually has a significant impact on the user's freedom of choice, independence, and ability to make a free, informed choice. A dark pattern can be a button that is highlighted, an option that is hidden, a prompt that appears repeatedly, a route to canceling the action that is confusing, an item added automatically, or a privacy setting that's hard to change. While these might be small practices in isolation, they do add up and make the online experience one where users are nudged towards the choices the platform desires.

One of the legal issues around dark patterns is that they manipulate the user and digital platform relationship. The architecture is controlled by the platform and the interaction is typically where the user has limited time, limited attention, limited technical knowledge and unequal access to the information. This imbalance enables digital platforms to influence consumer choices, get consent, gather information, make payment, hold back users to keep their subscriptions, or boost users' involvement in a manipulative design. Hence, a dark pattern analysis should be more than just a technical analysis of dark patterns and should also consider the impact that dark patterns have on the autonomy, privacy, consent and fairness of consumers.

4.1 Dark Patterns as Unfair Trade Practices

Dark patterns could be considered unfair trade practices as it hinders the consumer from making a free and informed commercial choice. In traditional consumer protection law, unfairness is typically linked to false representations, hidden costs, misleading marketing, forcing the sale on a consumer or to a consumer, or, failing to disclose material facts to a consumer. A similar unfairness can happen in a digital environment by means of interface design. A platform does not necessarily need to be making an express false statement in order to be considered to be misleading the consumer but may be misleading consumer by manipulating the way options, prices, terms and cancellation options are presented in the contract and consent mechanisms are obtained.

The problem with dark patterns from a legal perspective is that they deceive the consumer in making his choice. Examples of false urgency, basket sneaking, drip pricing, bait and switch, disguised advertisement and subscription traps have a direct impact on the fairness of online transactions. False urgency is the one that pushes the consumers with a sense of scarcity, of doing it urgently or in a hurry. Basket sneaking involves the addition of products, services, donations, insurance or other charges without any apparent consent. Don't be misled by drip pricing - this is when the total price of the transaction is hidden from the customer until the end of the process. Bait and switch: lures customers with an offer and then leads them to another. Subscription traps facilitate easy entry into a paid service, but make it hard to opt out. These practices are unfair, since they diminishthe consumer's ability to make a meaningful comparison and to appreciate the true price, and to make a free choice.

Legally speaking, dark patterns can be classified as recognised consumer protection types, depending on the type of design and its effect on the consumer (Isola and Esposito, 2025). These may include:

- **Misleading action:** where the interface gives a false or deceptive impression to influence the consumer’s decision.

- **Misleading omission:** where important information, such as price, cancellation rights, privacy consequences, or additional charges, is hidden or not clearly disclosed.
- **Harassment:** where repeated pop-ups, reminders, or interruptions pressure the consumer to act in a particular way.
- **Undue influence:** where the design exploits emotional pressure, urgency, fear, guilt, or information imbalance to influence the consumer.
- **Coercion:** where the user is forced to take an unnecessary action, such as sharing personal information or subscribing to a service, in order to proceed.

This classification can be helpful as it relates dark patterns to existing notions of consumer protection and not just as novel technology issues. For instance, a cancellation is not a cancellation if it is hidden or if there is repeated pop up or emotionally pressuring messages, then this is considered harassment or undue influence.

The Indian Guidelines for Prevention and Regulation of Dark Patterns, 2023, add further weight to this stance, by explicitly deeming dark patterns as adverse digital practices. The Guidelines identify 13 types of dark patterns: false urgency, basket sneaking, confirm shaming, forced action, subscription trap, interface interference, bait and switch, drip pricing, disguised advertisement, nagging, trick question, SaaS billing and rogue malware. These categories indicate that digital design, as a place where unfair trade practices can take place has now been recognised under Indian consumer protection law. The focus no longer has to be on the end sale or advertisement; it's on the whole online choice environment.

FTC's reasoning also applies as they consider dark patterns to be unfair or deceptive practices, as they trick consumers into giving away money or data. It is of great importance for legal analysis as it is established that the unfairness of a business can manifest itself not only in the content of what is said, but also in how an interface is designed. Examples of design-based unfairness are pre-ticked boxes, hidden disclosures, confusing cancellation procedures and unwanted additions to shopping carts.

The Indian legal academia is also cognizant of the grave issues that dark patterns pose in the digital economy for consumer protection. These practices take advantage of the fact that there is an information asymmetry between the platform and consumers, particularly when consumers lack time, knowledge, and/or negotiating power, and when the platform determines the interface's characteristics (Sharma, 2023; Chugh and Jain, 2021). Clicking on a button, or even making a transaction, could be considered a free and informed consent, if the interface is not designed to mislead, pressure or obstruct the consumer.

Thus, the analysis of dark patterns should focus on their effect on the ability of consumers to make their choices freely, to lack information, to pay an unwanted price, or to refuse/desist from unwanted actions or contracts. The key issue should not be whether or not information was in a way technically accessible somewhere on the platform. Instead, the law should require that the question be whether or not the information was presented in a clear, timely, accessible and neutral way. Where the design makes it easier to accept than to refuse, material facts are hidden or disclosure of price is delayed, or consumers are involved in transactions which they do not really want, there is a lack of fairness in the Digital Commerce.

4.2 Dark Patterns as Privacy and Consent Problems

Dark patterns are also a significant issue with respect to privacy and consent: digital services often require users to give consent to collect, process, store and share personal data and monetise that information. In digital context, cookies banners, app permissions, account settings, privacy dashboards, sign-up forms and subscription pages, and data-sharing pop-ups are a few common methods for obtaining consent. But, consent can only have a legal significance, if it is free, informed, specific and if it can, without unreasonable difficulty, be refused or withdrawn. Dark patterns undermine these conditions: by

making it easier to accept, more difficult to reject and more challenging to see privacy choices.

One of the typical examples is creating cookie consent banners. Many platforms will prominently show an "Accept All" button and may have the "Reject" or "Manage Preferences" button in several layers of menus that can be difficult to find. The same goes for mobile apps: permissions for various things (Location, contacts, notifications, tracking, etc.) may be repeatedly requested until the user gives them. In these scenarios, although there is perhaps an explicit form of consent, there is a question over the quality of the consent. Whether the user pushed a button is not all that matters, whether there was an opportunity for the user to make a free and informed choice is what matters.

There is an intersection between consumer protection and data protection law: the link between dark patterns and consent. Due to their potential to undermine the principles of fairness, transparency, privacy-by-design and valid consent, dark patterns should be addressed by consumer and data protection laws and regulations (Leiser, 2022). A manipulative interface can be misleading on the business side and also facilitate over- or unfairly processing personal information.

There can also be privacy harms that stem from dark patterns which are not readily apparent. These harms can be loss of control over personal data, unwanted tracking and profiling, targeted advertising, sharing personal data with third parties, cognitive overload, emotional stress and loss of autonomy. The literature on privacy harms suggests that the potential harms of dark patterns can be both material and non-material, and that data protection law should take into account whether there is a remedy available for these harms (Gunawan et al., 2022).

Consent scholarship also reveals that there is a need to view the entire consent process and not just the last step of clicking "agree." Whether consent is meaningful is influenced by the location of buttons, the number of steps required to deny consent, the language used for the options, the default choice, colour schemes of the buttons and repeated prompts. Some research into cookie consent requests suggests that interface design can have a significant impact on privacy choices and can lead consumers to privacy-disclosing options when designing the interface is more likely to lead them to accept than refuse (Graßl et al., 2025). Likewise, consent banner studies highlight the need to assess consent mechanisms in the legal, ethical, social and interaction-design lens (Gray et al., 2021).

An issue of consent fatigue is another one that has to be taken into account. Users are continually presented with banners, pop-ups, notifications and requests for permission and privacy statements. Users may over time opt out of reading these notices, and go for the fastest available option. Fatigue may be used to the platform's benefit as it makes the option that is less privacy-protective more convenient than the option that is more privacy-protective. If so, consent is not actually consent, but the lack of it is a result of exhaustion and/or convenience.

Recent legal research further reveals that the effects of dark patterns can be far-reaching and impact not just data protection law, but consumer law and competition law as well (Santos et al., 2025). A dark pattern that secures too much information from the users can at the same time be a violation of privacy interests, a manipulation of the free choice of the users, an increase in platform power and a decrease in market fairness. So, privacy and consent issues stemming from dark patterns are by no means a purely technical issue. They're part of a larger legal battle about the responsibility of platforms, the control of information and the autonomy of users.

So dark patterns go against the conventional notion that a user's consent can simply be presumed from a click on the "accept" button. When the surrounding interface provides no alternatives, or makes it difficult to refuse the consent, or uses language that is confusing, or presses the user a lot, consent is not considered to be completely free and informed. That's why the law needs to take a look at the consent landscape as a whole, and ensure it provides users

with meaningful, equitable, and easy access to control of their personal information.

4.3 Dark Patterns and Consumer Vulnerability

Dark patterns are closely linked with consumer vulnerability, since they capitalise on the circumstances in which consumers make their decisions in digital environments. Consumer protection law is traditionally based on the identification of vulnerable consumers through fixed categories, e.g. children, elderly people, consumers with disabilities, or economically weaker consumers. But dark patterns reveal that these groups aren't the only ones who are vulnerable. When a platform confuses, urges, pressures, tires or overloads with information, any user can be vulnerable.

Digital platforms set up the choice environment, determining what information is first in view, which choice is made more salient, how easy it is to cancel, or how easy it is to opt out of privacy-protective choices. This means that even knowledgeable/experienced users can be influenced. Based on these empirical studies, it seems that dark patterns can impact various groups of users and that it is not just traditionally vulnerable consumers that are susceptible to dark patterns (Zac et al., 2025). Vulnerability can also be due to contextual and technology issues like small mobile screen size, complex privacy settings, frequent pop-ups, saved payment information, one-click purchasing, and need for services (Rossi et al., 2024).

Dark patterns can thus be seen as a form of digital abuse for they make use of the power imbalance platform and users. Platforms have technical know-how, behaviour data, design control, and commercial incentives, whereas users typically have limited time, attention, and understanding of the impact of the interface on them (Boris et al., 2024). The legal reaction should thus be directed towards the impartiality of the digital choice environment, where platforms need to provide a neutral presentation of choices, a clear information policy, and an easy possibility to refuse, cancel or withdraw consent.

4.4 Dark Patterns and Platform Accountability

Another problem with dark patterns is that of platform accountability. Digital platforms are no longer just passive intermediaries but are the creators of the system by which users view information, consent, make purchases, adjust privacy settings, and cancel services. Platforms are responsible for controlling the architecture of digital choice and therefore have a responsibility to ensure that interfaces do not mislead, pressure, obstruct or manipulate users.

Platform accountability needs to be more than simply looking at express false statements. The design may be considered unfair even if a notice, privacy policy, or cancellation option is formally displayed because the notice is hidden, privacy policy is not readable, or the cancellation option is not easily accessible. Enforcement literature indicates that deceptive design may operate not only at the visible interface level but also within the underlying system architecture that shapes user behaviour (Leiser and Santos, 2023). Therefore, platform accountability should examine both front-end interface design and back-end system structures that influence user choices. The autonomy-based regulation approach is favored in this regard because it is important to be able to make a meaningful choice (Brenncke, 2024).

Practical accountability measures should include fairness-by-design principles, equality of visibility of both acceptance and rejection possibilities, ease of cancellation procedures, clarity with respect to extra charges, accessibility of privacy settings, no pre-ticked boxes, and ease of withdrawal of consent. In addition, the FTC's enforcement action demonstrates that companies can be held liable for charges they fail to disclose, confusing cancellation procedures, pre-checked boxes, unwanted cart add-ons and deceptive subscription offers. Dark patterns can inflict financial, privacy, autonomy, psychological and market harms (Santos et al., 2025) , thus supporting a broader accountability. Thus, responsibility of platforms that gain from creating digital choice environments should also

include the responsibility for maintaining a fair, transparent and non-manipulative environment.

4.5 Gaps in Existing Legal Framework

Although there is increasing attention being paid on dark patterns, there are still some aspects that are incomplete in legal frameworks. First, many of the laws were geared towards the old ways and means of deception such as false statements, misleading advertisements, or hidden costs. But dark patterns can be implemented using a variety of subtle features like visual hierarchy, default settings, concealed options for refusal, repeated prompts or unnecessary friction. Although there may not be any false statement, these practices could potentially influence user choice. Thus, the current legal framework has to be flexible enough to take on the issue of design-based manipulation as one that is worthy of regulation in its own right (Isola and Esposito, 2025; Leiser and Santos, 2023; Brenncke, 2024).

Secondly it might be hard to establish the damage of dark patterns. Financial damage is potentially more apparent when the user is paying behind the scenes or is paying for a subscription that they didn't want. But the harm to privacy, loss of autonomy, emotional stress and loss of control of personal information are more difficult to quantify. This poses an enforcement problem as the damage wrought by dark patterns can be non-material and/or diffuse (Santos et al., 2025).

Third, the practice of dark-patterns is still scattered. Consumer protection law, data protection law, (advertising) regulation, cyber law and competition law may all overlap with the same practice. This overlap may result in uncertainty as to which enforcement agency is the right one to pursue a claim, what the standard of proof is for such a claim, and what the remedy is. Therefore, from a legal point of view, a pluralist regulatory approach is advocated, a combination of consumer protection, data protection and the regulation of digital platforms (Leiser, 2022).

Fourth, there is a lack of the connection between formal disclosure and choice. While there are many platforms that offer information, privacy policies, banner and cancellation rights, the layout may make it difficult to exercise these rights. It is therefore vital to evaluate legal compliance not just with regards to the existence of information, but also the clarity, accessibility, timeliness and neutrality of the information (Isola and Esposito, 2025).

Fifth, in the Indian context, the recognition of thirteen dark patterns is a significant development, but effective enforcement remains essential. Regulatory bodies need technical capacity to detect manipulative interfaces, audit digital platforms, assess consent flows, and monitor compliance. Indian legal scholarship further shows that dark patterns should be examined within the broader framework of e-commerce, consumer protection, information asymmetry, and digital market regulation (Sharma, 2023; Chugh and Jain, 2021).

Finally, there are many issues with crossborder enforcement. Many platforms are available across international borders and users, data, servers, as well as contractual terms, may be in different countries. Thus, there is a need for regulatory coordination, particularly for the issues of personal data, targeted advertising, online payment and digital transactions, where dark patterns occur. Looking forward, future policies should be comprehensive, incorporating greater legal clarity, technical enforcement capabilities, consumer remedies and holding platforms liable. Table 4 summarises the main legal harms caused by dark patterns and the possible remedies available to address them.

Table 4: Legal Harms Caused by Dark Patterns

Type of Harm	Related Dark Pattern	Legal Issue	Possible Remedy
Financial harm	Drip pricing, basket sneaking, SaaS billing	Hidden charges, unwanted payments, unfair billing	Refund, penalty, compensation, clear price disclosure
Privacy harm	Forced action, interface interference, cookie consent manipulation	Invalid consent, excessive data collection, misuse of personal information	Data protection complaint, withdrawal of consent, privacy-by-design compliance
Autonomy harm	Confirm shaming, trick questions, false urgency	Manipulated choice, pressure-based decision-making	Interface redesign, regulatory directions, prohibition of manipulative prompts
Contractual harm	Subscription trap, bait and switch	Unfair contract terms, difficult cancellation, misleading offer	Easy cancellation, cancellation rights, consumer redress
Psychological harm	Nagging, fear-based prompts, rogue malware	Stress, fatigue, fear, emotional manipulation	Enforcement action, design standards, user protection measures
Market harm	Disguised advertisement, misleading rankings, manipulative platform design	Reduced transparency, unfair competition, distorted consumer choice	Advertising disclosure, platform audits, competition and consumer enforcement

These tables show that dark patterns require a combined consumer protection, data protection, and platform accountability response.

5. Conclusion

Dark patterns has turned into a legal and regulatory issue in the digital realm. Not only are they questionable design decisions, but they are problematic interface practices that impact consumer autonomy, informed consent, privacy and the fair use of personally collected information. Digital platforms can have an impact on users' decision-making processes by employing various methods, including false urgency, basket sneaking, subscription traps, interface interference, forced action and disguised advertisements.

The study reveals that dark patterns can be considered as an intersection of consumer protection, data protection, advertising regulation and digital governance. They can have financial, privacy, autonomy, contractual, and psychological impacts. While the Guidelines for Prevention and Regulation of Dark Patterns are a critical step taken by Indian law, enforcement and platform responsibility are key.

Transparency, a neutral user interface design, ease of cancellation, meaningful consent and easy access to privacy controls are essential for a fair digital environment. There is therefore a need to shift away from 'notice' and to understand if the digital choice environment enables free, informed and autonomous decisions to be made.

References

Boris, E., Ksenia, K. and Natalia, S. (2024) Digital abuse: How dark patterns manipulate our lives. *Legal Issues in the Digital Age*, No. 4, 4–27.

Brenncke, M. (2024) Regulating dark patterns. *Notre Dame Journal of International & Comparative Law*, Vol. 14, 39.

Central Consumer Protection Authority. (2023) Guidelines for prevention and regulation of dark patterns, 2023. Department of Consumer Affairs, Government of India. Available at: https://doca.gov.in/ccpa/guidelins.php, accessed May 2025.

Chugh, B. and Jain, P. (2021) Unpacking dark patterns: Understanding dark patterns and their implications for consumer protection in the digital economy. *RGNUL Student Research Review Journal*, Vol. 7, 23.

Federal Trade Commission. (2022) Bringing dark patterns to light: An FTC staff report. Available at: https://www.ftc.gov/reports/bringing-dark-patterns-light, accessed May 2025.

Graßl, P., Schraffenberger, H., Borgesius, F. Z. and Buijzen, M. (2025) Dark and bright patterns in cookie consent requests. *arXiv preprint* arXiv:2509.18210.

Gray, C. M., Bielova, N., Santos, C. and Mildner, T. (2024) An ontology of dark patterns: Foundations, definitions, and a structure for transdisciplinary action. In *Mitigating Dark Patterns Through Responsible Design*, 171.

Gray, C. M., Kou, Y., Battles, B., Hoggatt, J. and Toombs, A. L. (2018) The dark (patterns) side of UX design. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*, 1–14.

Gray, C. M., Sanchez Chamorro, L., Obi, I. and Duane, J. N. (2023) Mapping the landscape of dark patterns scholarship: A systematic literature review. In *Companion Publication of the 2023 ACM Designing Interactive Systems Conference*, 188–193.

Gray, C. M., Santos, C., Bielova, N., Toth, M. and Clifford, D. (2021) Dark patterns and the legal requirements of consent banners: An interaction criticism perspective. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*, 1–18.

Gunawan, J., Santos, C. and Kamara, I. (2022) Redress for dark patterns privacy harms? A case study on consent interactions. In *Proceedings of the 2022 Symposium on Computer Science and Law*, 181–194.

Isola, C. and Esposito, F. (2025) A systematic literature review on dark patterns for the legal community: Definitional clarity and a legal classification based on the Unfair Commercial Practices Directive. *Computer Law & Security Review*, Vol. 58, 106169.

Kollmer, T. and Eckhardt, A. (2023) Dark patterns. *Business & Information Systems Engineering*, Vol. 65, No. 2, 201–208.

Leiser, M. and Santos, C. (2023) Dark patterns, enforcement, and the emerging digital design acquis: Manipulation beneath the interface.

Leiser, M. R. (2022) Dark patterns: The case for regulatory pluralism between the European Union's consumer and data protection regimes. In *Research Handbooks in European Law*, E. Kosta, R. Leenes and I. Kamara (eds), Edward Elgar Publishing, Cheltenham, 240–269. doi: 10.4337/9781800371682.00019.

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*, Vol. 3, No. CSCW, 1–32.

Rossi, A., Carli, R., Botes, M. W., Fernandez, A., Sergeeva, A. and Chamorro, L. S. (2024) Who is vulnerable to deceptive design patterns? A transdisciplinary perspective on the multi-dimensional nature of digital vulnerability. *Computer Law & Security Review*, Vol. 55, 106031.

Santos, C., Morozovaite, V. and De Conca, S. (2025) No harm no foul: How harms caused by dark patterns are conceptualised and tackled under EU data protection, consumer and competition laws. *Information & Communications Technology Law*, Vol. 34, No. 3, 329–375.

Sharma, J. (2023) Dark patterns in a bright world: An analysis of the Indian consumer legal architecture. *IJCLP*, Vol. 11, 123.

Zac, A., Huang, Y. C., Von Moltke, A., Decker, C. and Ezrachi, A. (2025) Dark patterns and consumer vulnerability. *Behavioural Public Policy*, 1–50.