KMANPUB | AI and Tech in Behavioral and Social Sciences Vol. 4 No. 2 (2026): 1-13

Article history:
Received 26 August 2025
Revised 26 September 2025
Accepted 25 November 2025
Published online 01 April 2026

Examining Iran's Business Laws: Protecting Against Soft Technology Abuse in Digital Platforms

Rasoul Jamshidi[1*], Sattar Rajabpour Sanati[2]

[1] Department of Industrial Engineering, School of Engineering, Damghan University, Damghan, Iran
[2] Department of Industrial Engineering, Iran University of Science and Technology, Tehran, Iran

*** Corresponding author email address**: r.jamshidi@du.ac.ir

A r t i c l e I n f o

Article type:
Review Article

How to cite this article:
Jamshidi, R., & Rajabpour Sanati, S. (2026). Examining Iran's Business Laws: Protecting Against Soft Technology Abuse in Digital Platforms. *AI and Tech in Behavioral and Social Sciences, 4*(2), 1-13.
https://doi.org/10.61838/kman.aitech.4551

A B S T R A C T

In today's digital economy, maintaining a competitive advantage has become increasingly important for businesses, leading them to adopt various means to attract customers to their products and services. One of the tools gaining more attention recently is the use of soft technologies and persuasive systems, which can be applied in digital and non-digital fields, particularly in e-commerce businesses to mask product weaknesses and emphasize competitive advantages, thus encouraging customers to buy. The study aims to investigate the risks associated with soft technologies, such as psychological pressure and the exploitation of vulnerable individuals, as well as to review the status of Iran's business laws that can protect people from these harms. This applied research utilizes the onion research model. The findings suggest that Iran's commercial laws fall short of international standards in protecting people from deceptive and persuasive designs. As a result, we made several recommendations to improve Iran's commercial laws.

Keywords: *Persuasive System Design (PSD), Dark Patterns, Deceptive Design, Consumer Protection Law, Data Protection Law*

1. Introduction

In the digital age, we spend more time and resources interacting with digital technologies than ever before. Technology companies not only provide us with useful services but also deliberately try to "enter our thoughts and minds" and "win the attention race" (Berthon et al., 2019). Technology companies design devices and applications to maximize "screen time" and "user engagement," often referred to as "usability and visual appeal." Social media companies exploit cognitive biases, like gamification, to make their platforms more addictive, by implementing algorithms to generate sensational content and using personalization and misinformation to create distractions tailored to each user (Hanin, 2021; Marin, 2021; Specker Sullivan & Reiner, 2021). The term "attention economy" refers to a business model in the technology industry that views human attention as a valuable resource. Concerns over the impact of persuasive technologies (PT), such as smartphones, social media platforms, and methods of gamification on the quality of human attention, have increasingly become an ethical concern (Zheng, 2024). Studies in the field of attention economy have revealed that these technologies can cause addiction and negative effects

on our brain function (Firth, 2019). The World Health Organization (W.H.O) recently added "gaming disorder" to its list of behavioral addictions, highlighting the potential dangers associated with digital technologies. Designing for addiction is just one example of the "ledger of harms" linked to digital technologies, which also include increased political polarization, risk-taking behavior, and decreased mental health (Pontes et al., 2021).

The development of the Fourth Industrial Revolution and digital technologies, such as the Internet of Things (IoT) and customized software, has brought many benefits to better manage resources, increase efficiency, and provide convenience for individuals and organizations (Rajabpour Sanati et al., 2024). However, this rapid growth of digital technologies also increases potential vulnerabilities, such as data privacy breaches (Gutta, 2024). While it is impossible for modern society to completely avoid interaction with digital technologies that use persuasive soft techniques, people must adapt to new norms. These technologies often generate worthless resources, leading to political and ethical concerns. Therefore, the attention economy can be seen as socially disruptive (de Laat, 2019; Hopster, 2021). The ethical implications of persuasive technologies and digital platforms tend to be narrowly framed around privacy and data protection, neglecting issues of autonomy, dignity, and power dynamics. This limited perspective fails to consider non-Western viewpoints, limiting the breadth of critique and potential solutions. Contrastingly, Eastern perspectives like Buddhist ethics emphasize the inherent ethical and ontological embeddedness of our attention. According to this perspective, the solution to face PT is to emphasize mindfulness, correct effort, and concentration to better pay attention to life's direction. However, the libertarian critique of attention economy business models, which prioritizes individual control, may not align with non-Western perspectives (Bombaerts et al., 2023).

The aim of this study is to examine Iran's commercial laws as potential preventive mechanisms against cases of soft technology abuse, comparing them with global actions in this context.

2. Literature and Research Review

Technology can generally be divided into two categories: "soft" and "hard" technologies. With technological advancement and economic development, the line between them is becoming more blurry. Soft technology refers to the intellectual technology of creation, innovation, and thought, focusing on ideology, feelings, values, worldviews, individual and organizational behaviors, and human society. Science is knowledge, while technology is ability. Technological ability can be defined as "the ability to convert input into a certain output". The key difference between soft and hard technologies is (Rajabpour sanati & Jamshidi, 2025):

- In hard technology, the input lacks will and authority (e.g., Nano, laser, Nuclear)
- In soft technology, the input possesses will and authority (e.g., individuals, groups, organizations)

To clarify the difference between hard technology and soft technology, we have listed some of the characteristics of these two concepts in Table 1 (Rajabpour sanati & Jamshidi, 2025).

Table 1

Overview of the differences between hard technology and soft technology

Criteria	Hard technology	Soft technology
Operational goal	Material	Human physiological functions and social behavior
Operational area	The physical world	The world of thought and mind
Operational ideal	Changing and controlling the nature and essence of matter	Dominating, organizing, and managing the ideology, emotions, way of thinking, values, and behavioral states of individuals, groups, and organizations
Source	Knowledge derived from natural sciences	Knowledge derived from unnatural and non-traditional sciences
Innovation process	Processing raw materials for product manufacturing, product design, production and marketing	Original/abstract idea, different formal systems/different models/methodology, implementation, regularization; system and methodology design, launch/implementation, process development from which new rules emerge, replacement of the old system, creation and construction of a new system
Problem solving method	Goods and services	Processes, laws, rules

AITBSS
AI and Tech in Behavioral and Social Sciences
E-ISSN: 3041-9433

In summary, soft technology aims to guide the motivations and will of individuals to achieve a desired outcome in an efficient and cost-effective manner. This aligns with the concept of persuasive technologies (PT), which are designed to influence user behavior without employing any form of coercion or force (Fogg, 2002). Persuasive system design (PSD) in digital term, refers to the design of information systems that can influence users' attitudes, behavior, or decision-making, either positively or negatively. On the one hand, PSD can help users achieve desirable outcomes by motivating them to make positive changes. On the other hand, if used unethically, PSD can lead to users disclosing unnecessary information or agreeing to unfavorable conditions, negatively impacting their well-being (Benner et al., 2022). However, persuasive technology is broadly defined as technology that is used to change the attitude or behavior of users through persuasion and social influence, while soft technologies encompass a broader spectrum and are used to change user behavior through influencing emotional, sentimental, and even coercive dimensions (Rajabpour sanati & Jamshidi, 2025). Here are some examples of soft tools and techniques for behavior change:

- Nudging: a gentle method of guiding users toward a desired behavior through subtle cues and social norms (Banerjee & John, 2023).
- Gamification: the use of game mechanics in non-game contexts to motivate and engage users (Stieglitz et al., 2017).
- Gamblification: This term refers to the use of design elements associated with gambling, such as lottery tickets, scratch cards, or loot boxes, in non-gambling contexts to increase user engagement. This can include features like random rewards or small wins, which are known to stimulate the brain's reward system and can be quite addictive (Adam et al., 2022; Macey & Hamari, 2024).

In recent years, persuasive tools have successfully been implemented across various sectors, from education to e-health to e-government. However, their potential to influence users raises ethical concerns, as these technologies could disrupt user autonomy and lead them to goals set by system designers. This could result in unethical decision-making processes and negative consequences for users, such as psychological and emotional harm. These new technologies allow designers to influence users' decisions, collect data, and even manipulate users into unethical outcomes (Benner et al., 2022). Reviewing studies on the ethical aspects of systems that use soft technologies reveals a range of ethical values, including privacy, trust, autonomy, informed consent, accountability, and sustainability. Considering these values when designing information systems is known as value-sensitive design (Schmidt, 2020; Spiekermann et al., 2022). The vastness and ongoing scholarly debates within the field of ethics make it difficult to cover every area of concern. To focus on the most prominent areas of ethical considerations in the literature, we will concentrate on three key areas (Benner et al., 2022):

2.1. Infringement of Individual Autonomy and Freedom of Choice

The first ethical assumption is that any intervention should be easy for users to avoid, for example, by clicking a button. In order for an intervention to be ethical, it must preserve an individual's freedom of choice, avoiding any perception of coercion or restriction. Real freedom of choice exists when people are able to make rational decisions without third-party limitations (Sugden, 2009).

The second ethical assumption is violating transparency can infringe upon individual independence and freedom of choice. When the options available to users are obscured, the decision made could endanger their freedom. Therefore, to maintain freedom of choice, it's essential that users are able to easily recognize when and where they're being influenced by nudges or other soft mechanisms (Lembcke et al., 2019).

2.2. Goal-oriented Justification: A Means to an End

Soft persuasive technologies can be designed with different goals. After reviewing systems based on these technologies, their goals can be broadly classified into the following areas(Clavien, 2018; Hagman et al., 2015; Lembcke et al., 2019):

1. Selfish goals of the designer at the expense of users' satisfaction (e.g., profit)
2. Social goals (e.g., public welfare, gender equality)
3. Selfish goals of the designer that also satisfy users voluntarily (e.g., encouraging voluntary participation in sports activities).

The goals of each system can be placed in one or more categories. According to Dr. Thaler and Sunstein, there is no moral justification for the first goal in particular (selfishness), because a selfish perspective does not

AITBSS
E-ISSN: 3041-9433

necessarily influence people's behavior to make their lives longer, healthier, and better (Sugden, 2009).

2.3. *Invasion of Privacy*

Soft technologies, especially Digital nudges, through subtle changes in software and digital designs, can influence users to perform the designer's desired action. An example of such a design is cookie banners on websites, which often contain unethical pre-selected settings that force users to agree to unfavorable conditions that may violate their privacy (Özdemir, 2020). Additionally, unethical use of these technologies can result in the disclosure of sensitive user data on social media, leading to psychological and emotional harm (Kroll & Stieglitz, 2021). The primary purpose of such designs is to obtain more information from users for the benefit of the website designer, which is in conflict with the main concept behind using these tools: to create the 'greater good' for users (van den Hoven, 2021).

Although designers may have good intentions, such systems can lead to a morally questionable mindset. Some users may even voluntarily adopt unethical mechanisms that are specifically designed to induce them into certain behaviors or decisions, such as disclosing personal information, agreeing to unethical terms, or purchasing unwanted items. Researchers refer to these exceptionally unethical and even malicious designs as "dark patterns", a type of design that solely aims to maximize the benefits of the system designer (Kollmer & Eckhardt, 2023). However, policymakers and government institutions (e.g., the Chinese government) have recently identified potential challenges, threats, and opportunities associated with these mechanisms (e.g., the use of behavioral design for public policies). As studies on this topic are still in their infancy, more research is needed to better understand the ethical implications of such mechanisms (Kuehnhanss, 2019).

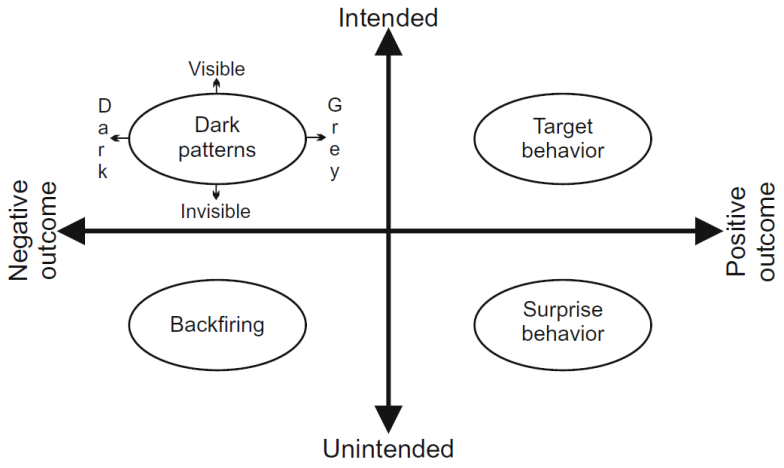
2.4. *Abusive Designs and Misuse of Soft Technologies*

If we classify user behavior based on its alignment with the designer's goal and its resulting benefits or harms, we can create a diagram as shown in Figure 1, where (Nyström & Stibe, 2020):

- The vertical axis indicates the degree to which the user's behavior aligns with the designer's goal (desired vs. unwanted behavior)
- The horizontal axis indicates the consequences or benefits for the user (positive vs. negative)

Figure 1

Type of system design (Nyström & Stibe, 2020)



In the left half of the diagram, which shows behaviors with negative consequences for users interacting with the system, we have two categories of systems (Nyström & Stibe, 2020):

a) Systems that, despite their positive intentions, evoke negative feelings and emotions in users, resulting in unwanted behaviors and negative consequences for the user. In this situation, both the designer's and the user's interests are at risk (Backfiring).

b) Systems that are intentionally designed to benefit the designer, often by using "dark patterns" that unfairly distribute benefits between the user and the

AITBSS
E-ISSN: 3041-9433

designer, or even exclusively benefit the designer (Dark patterns). To sum up, "dark patterns" can be broadly categorized as follows:

I. Gray-Visible; in this category, the system seems beneficial to users at first glance, but potential negative side effects are not clearly presented. While the benefits and potential benefits are emphasized, other potential side effects that may not be beneficial to users are less clear. This creates an ambiguity in the user's understanding, resulting in an unfair distribution of benefits between the designer and the users. For instance, loyalty reward systems, such as frequent flier rewards, may use such patterns.

II. Gray-Invisible; this category includes systems with features whose benefits may not be fully apparent or understood by users. As with the previous category, these designs skew benefits towards designers at the expense of users. Not only are the benefits biased, but also these systems try to disguise their goals by presenting misleading interactions with users. An example of such a pattern can be found in a mobile game called Two Dots. When a user loses the game, pressing a big green button means wanting to continue the game. However, when all available lives are gone, the user will see a familiar green button, but this time it means paying US$0.99 to continue!

III. Dark-Visible; this category includes systems that may create suspicion for users about the system's purpose. For example, Electronic Arts designed the FIFA soccer video game to include "loot boxes" that can be purchased by players to increase their chances of winning. The content inside the boxes is randomized, and many users claim that they must purchase loot boxes to stay competitive. They argue that the game design is "pay-to-win" and unfair, and some even develop gambling-like addictions that lead them to spend a lot of money on loot boxes.

IV. Dark-Invisible; in this category, the system is designed in such a way that its purpose is not only opaque to users but also potentially very harmful. This is where the darkest patterns hide because they are not only harmful from the user's perspective but also effectively disguised. These designs take advantage of inherent human weaknesses or cognitive errors. For example, Zynga produces Facebook games like FarmVille that allow players to make in-app purchases to gain in-game benefits.

Research on dark patterns reveals that these systems lead consumers to make decisions they may regret or not fully understand. Hiding information, trick questions, blocking strategies, and the 'Bandwagon effect' are particularly effective in manipulating customer decisions. On the other hand, 'act now' messages are not effective in persuading consumers to buy expensive services (Luguri & Strahilevitz, 2021). Therefore, the question arises: have laws been enacted to prevent such destructive designs and the resulting damages? In this study, we investigate the current state of international and Iranian laws in relation to violations of moral boundaries by such systems.

3. Methodology and Research Strategy

The Research Onion model, originally developed for business research, is now being widely adopted by researchers in diverse disciplines, including information systems. Since information, system is a field that combines social and natural sciences, modifications to the model are necessary to accommodate the various research methods and approaches used in information systems. Therefore, in this study, we use the modified Research Onion proposed by Mardiana, which incorporates IS research methods (Mardiana, 2020). Critical research, which is a type of comparative research based on archival research, is the appropriate philosophical approach for this study. In terms of objective, this research is 'applied,' meaning it is aimed at solving a specific problem. The main questions of this study will be:

- Do any global laws exist to prevent harm caused by dark patterns?
- Do Iranian commercial laws provide any mechanisms for preventing harm caused by dark patterns? If so, what are they and to what extent do they apply?

AITBSS
AI and Tech in Behavioral and Social Sciences
E-ISSN: 3041-9433

Table 2

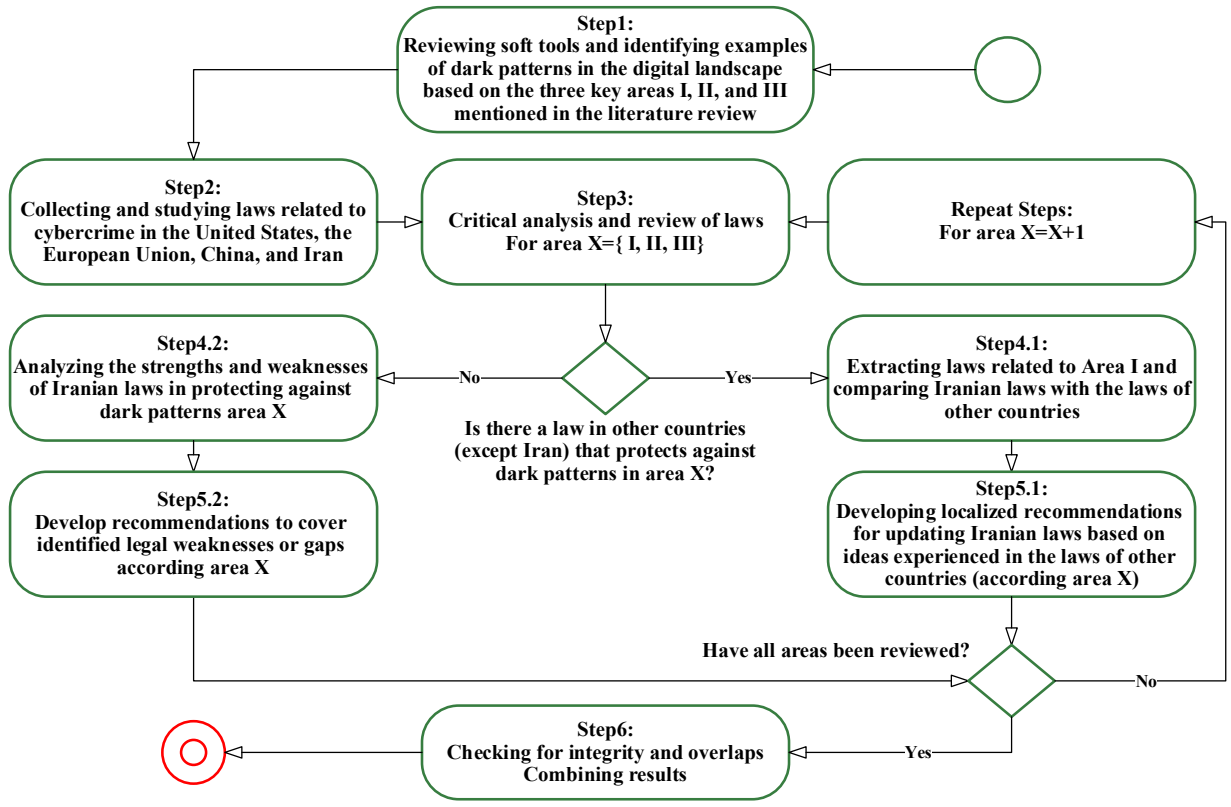
The research characteristic

The onion layer of research	Research characteristic	Description
Philosophy	Critical realism	A critical review of Iranian laws regarding the coverage of dark patterns in the digital context
Approach	Deductive	It comes from putting together accepted reality (laws passed in the context of dark patterns in other countries) and deducing a conclusion from it
Methods	Qualitative	Data is less likely to be converted into numbers, so it is analyzed in the same form in which it was collected.
Strategy	Archival research	Given the wide range of specialized legal issues, this study discusses some of the laws around the world that regulate soft technologies and related ethical violations. The United States, China, and the European Union are examined as major and leading economies in this field.
Time horizon	Cross- sectional	The time horizon is cross- sectional and relates to laws approved and valid in 2024.
Data collected	Non-Numerical	The data is descriptive and cannot be analyzed using statistical and numerical methods.

Table 2 lists the characteristics of the research methodology and the limiting criteria at the stages of research implementation. To elucidate the procedural details, the workflow of the research is decomposed into six principal steps, with three iterations between step 3 to step 5, as depicted in Figure 2.

Figure 2

Research steps flowchart



AITBSS
E-ISSN: 3041-9433

4. Review and Discussion

4.1. Review on global laws

Due to the broad scope of specialized legal issues, we briefly discuss some existing laws worldwide that regulate soft technologies and related ethical violations. As major economies and leaders in this sector, the United States, China, and the European Union were examined, and examples of relevant laws in these countries are discussed below.

4.1.1. United States of America (USA)

Several legal frameworks exist in the USA to limit dark patterns in e-commerce. First, the Federal Trade Commission (FTC) Act restricts unfair or deceptive practices in interstate commerce and directs the Commission to regulate and restrict such conduct. Second, state unfair competition laws have similar restrictions. The FTC's provisions to combat unfair and deceptive practices (under Section 5 of the FTC Act) are a clear legal entity that can regulate dark patterns. The FTC's investigative and enforcement powers cover all entities engaged in or affecting commerce (with a few exceptions). For example, one of the major controversial questions in these laws is (Luguri & Strahilevitz, 2021):

"Should consumer consent obtained through highly effective dark patterns be considered invalid?"

The FTC grants consumers the right to various remedies under contract law and can hold companies accountable for engaging in practices such as monitoring personal data or processing biometric information without proper consent. An FTC enforcement action against payday lender Scott Tucker provides an example of how dark patterns can be used to deceive customers. Tucker's websites disclosed loan fees in TILA (Truth in Lending Act) statements, but an important warning was hidden in the fine print. The warning offered two repayment options: "no renewal" or "renewal," which allowed borrowers to delay repayment at additional cost. Tucker's companies technically fulfilled their legal obligation to disclose loan terms (TILA), but the repayment page was designed to nudge customers toward the more costly renewal option. By burying the "No Renewal" option in the fine print, customers were more likely to select renewal unknowingly, potentially incurring additional costs. This use of a dark pattern violated consumer protection laws (Luguri & Strahilevitz, 2021). This law requires that, besides offering the necessary choices for exercising the right to choose, the options be presented in a clear and transparent manner to prevent influencing the decision and the emergence of cognitive biases.

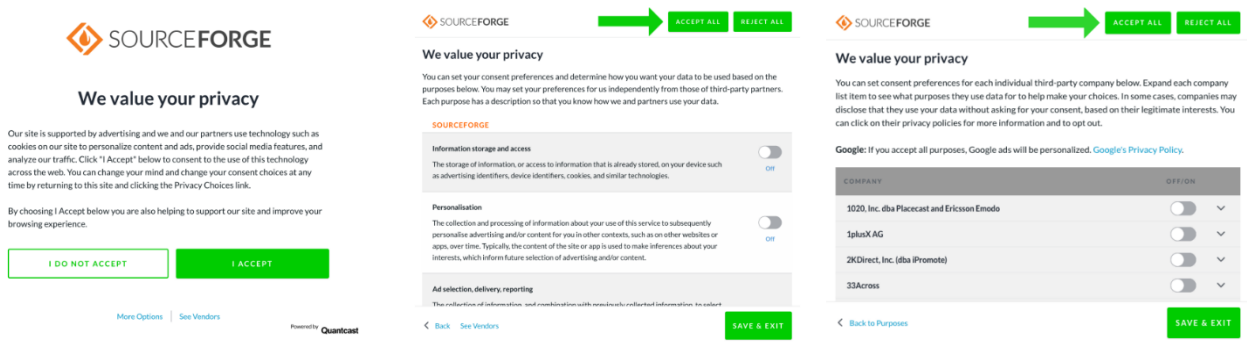
4.1.2. European Union (EU)

The EU's General Data Protection Regulation (GDPR) has highlighted the illegality of dark patterns that manipulate "notification and consent" in the EU. EU law focuses on the quality of consent required, emphasizing its voluntary and informed nature. To comply with GDPR, website owners often use Consent Management Platforms (CMPs) to outsource regulatory compliance. In 2018, the EU Data Protection Act repealed the 1995 Data Protection Directive and replaced it with the ePrivacy Directive, which contains new provisions for data protection and privacy (Nouwens et al., 2020):

- Free and unambiguous consent from the user
- Consent for a specific and informed matter
- Efficient protection and timely consent for data

Figure 3

An example of design considerations for Consent Management Platforms (CMPs) (Nouwens et al., 2020)



AITBSS
AI and Tech in Behavioral and Social Sciences
E-ISSN: 3041-9433

Figure 3 depicts the evolution of consent management platforms from a binary "Accept/Decline" decision (left) to a nuanced set of options enabling users to "Accept all" or "Accept some" cookies (right). Consequently, the implementation of this mechanism mitigates two related dark patterns risks: (i) coercive or fraudulent acquisition of user consent, and (ii) the collection of unnecessary data, whether during the initial consent process or in subsequent visits.

4.1.3. China

As an example of non-digital soft technology regulations, Shanghai's mandatory compliance guidelines for the use of blind boxes are worth mentioning. While blind boxes are popular with young consumers, legal gaps in this industry can lead to consumer rights violations and negative public sentiment. Blind boxes are new products that function as a form of gambling, as consumers pay to receive random content. In January 2022, Shanghai's Mandatory Compliance Guidelines and Guidelines for Using Blind Boxes in Marketing were published to protect consumers and limit gambling-related harms. These measures include publishing the probability of winning and implementing a "pity mechanic" that guarantees that consumers will receive at least the content they expect after making a specified number of purchases (Xiao, 2022; Zhang, 2024).

Figure 4

An example of blind boxes in the sale of collectible toys

Figure 4 depicts a toy box that, with each purchase, randomly yields one of eight dolls in the set. This blind-box design encourages repeat purchases as consumers strive to collect all dolls. The same approach could also be used for products that include lottery cards to encourage more purchases and improve odds of winning. Consequently, legislators have enacted requirements intended to reduce the risk of consumers being drawn into a vicious cycle of repeated purchases and to guarantee a quantifiable probability that consumers attain their intended outcomes.

4.2. Review on Iran laws

Most of Iran's business laws are very old, addressing violations of moral boundaries in a traditional manner, rather than the way we discussed previously. For example, the role of independence and freedom of choice is mentioned in Article 64 of the Business Guild Act of Iran. The definition of fraud and deception is limited to the seller's declaration and compliance with the specifications of the goods or services (Article 59 of the Business Guild Act of the country). Regarding privacy and information collection, intentional behaviors such as cyber-attacks and the destruction of information are addressed in the laws of electronic commerce and computer crimes. Table 3 shows the laws related to deception and abuse of soft technology in Iran.

AITBSS
AI and Tech in Behavioral and Social Sciences
E-ISSN: 3041-9433

Table 3

Overview of the laws related to deception and abuse of soft technology in Iran

law	Approval date	Related part	Areas
Business Guild Act (Iran, 2004a)	2004-03-14	Article 58 - Short selling: It means offering or selling goods or providing services below the prescribed amount or standard.	(II)
		Article 59 - Fraud: It means offering or selling goods or providing services that do not match the specifications of goods or services expressed or requested in terms of quality or quantity.	(II)
		Article 64 - Forced sale: It is the forced sale of one or more types of goods or services along with other goods or services.	(I)
e-Commerce law (Iran, 2004b)	2004-01-07	Chapter 3 - Topic 1 - Chapter 2 - Rules of Advertising (Marketing)	(II)
		Chapter 3 - Topic 2 - Chapter 2 - Protection of Trade Secrets	(III)
Law of computer crimes (Iran, 2009)	2009-05-26	Chapter 1 - Topic 1 - Unauthorized access	(III)
		Chapter 1 - Topic 2 - Unauthorized eavesdropping	(III)
		Chapter 1 - Topic 3 - Computer espionage	(III)
		Chapter 2 - Topic 1 - Computer forgery	(I), (III)
		Chapter 2 - Topic 2 - Destruction and disruption of data or computer and telecommunication systems	(II)
		Chapter 3 - Theft and fraud related to computers	(II)
		Chapter 4 - Crimes against chastity and public morals	(II)
		Chapter 5 - defamation and publication of lies	(II)

Guide: (I) Infringement of Individual Autonomy and Freedom of Choice, (II) Goal-oriented Justification: A Means to an End, (III) Invasion of Privacy

In Iran, digital users' information is easily collected and sold without their consent, leading to unwanted promotional messages and other abuses. Iranian laws lack the necessary deterrents to prevent businesses from repeatedly using and selling user information (Nazari, 2025; SharghMediaGroup, 2025). While we saw in the examples of American and European laws that abuse of cognitive errors of users (consumers) to encourage them to make a specific choice is also an example of deceptive and fraudulent violation. In short, studies show that there are these problems in Iran's laws:

- The issue of privacy rights enforcement is unclear, as there are no clear guidelines on how a person can exercise their rights or under what conditions they can do so.
- While some businesses and IT service providers are required to retain certain data categories for defined periods, there are legal gaps in how this data is protected or used. For example, Articles 32 and 33 of the Computer Crimes Act require service providers to retain traffic data for at least six months and storage data for at least fifteen days after service termination. Yet there is no explicit requirement on data deletion timelines or on privacy protections and data-subject rights. Although Article 59 of the E-Commerce Act, and Articles 1, 2, and 3 of the computer crimes Law appears to recognize the right to data deletion and to require user consent for data-use purposes, in practice the provisions face complexities that hinder their full implementation. For instance, security considerations can override user consent, and government agencies may not consistently respect these rights. A related concern is the processing of user behavioral data in cyberspace, which is not always collected directly from users but may be inferred from their online actions.
- Although Articles 58 and 59 of the E-Commerce Law require consent for the use of personal data, regulation of data brokers—those who collect and sell citizens' data without a direct contractual relationship—remains insufficient. Many organizations harvest data from social networks without any obligation to inform data subjects. For example, social listening firms process large volumes of user data across multiple platforms without notifying individuals or securing consent. Moreover, some practices rely on vague or blanket consents, thereby circumventing the restrictions imposed by Articles 58 and 59.
- The law does not provide additional legal protections for vulnerable groups, especially children, regarding privacy (Articles 35 and 57 of the E-Commerce Law).
- While the implementing regulations for Articles 32 and 48 of the E-Commerce Law have been

AITBSS
E-ISSN: 3041-9433

prepared and approved, the regulatory framework governing other related provisions, notably those emphasized in Article 79, remains unclear.

- There are no codified obligations for businesses around managing personal data and the way of informing individuals about it.
- Businesses are not required to report data leaks to the relevant authorities or individuals.
- Outdated laws that do not address dark patterns or modern digital design practices.
- Limited definition of fraud and deception in business laws.

4.3. *Examples of Legal Cases Regarding Deceptive and Destructive Soft Technologies*

Despite the absence of domestic cases in Iran, Dr. Harry Brignull and his team have compiled a wealth of international legal cases and fines related to dark patterns at www.deceptive.design. The website was founded in 2010 to expose unethical design practices, educate the public, and promote digital awareness (Brignull & Darlo, 2010). These efforts have contributed to new laws such as the EU's Digital Services Act (DSA) and California Privacy Rights Act (CPRA). The issue has also gained traction with legislators and digital experts. Some notable examples of legal cases and their fines are included below. For more information about each of them and to view other legal cases, you can refer to Dr. Brignull's website (Brignull, 2024).

4.3.1. *Case 1: Epic Games*

The company was fined by the FTC for allegedly using deceptive techniques to coerce players into making unwanted purchases, as well as tricking children into spending money without parental consent.

- Fine: $245 million
- Location: USA
- Supervisory authority: FTC
- Legal basis: Children's Online Privacy Protection Act Rule, 15 U.S.C. §§ 6501-6506
- Case number: Docket No. C-4790
- Date: March 13, 2023

4.3.2. *Case 2: TikTok*

TikTok was fined by the France's Commission Nationale de L'Informatique et des Libertés (CNIL) for using advertising identifiers without user consent and having a cookie banner with insufficient information. The banner was designed to accept all cookies with one click and made it difficult to reject them, even placing advertising cookies on the user's browser if they did not accept them.

- Fine: €5,000,000
- Location: European Union and United Kingdom
- Supervisory authority: CNIL
- Legal basis: French Data Protection Act - Article 82
- Case number: Délibération SAN-2022-027 du 29 décembre 2022
- Date: December 29, 2022

4.4. *Case 3: Amazon Europe Core*

The French CNIL found Amazon guilty of using cookies without prior consent and not informing users on how to accept or reject them.

- Fine: €35 million
- Location: European Union and United Kingdom
- Supervisory authority: CNIL
- Legal basis: French Data Protection Act - Article 82
- Case number: Commission File No. 000-22513
- Date: June 27, 2022

4.4.1. *Case 4: Google LLC*

The Irish DPC found Google guilty of using a cookie notice that did not allow users to easily reject cookies by not providing a "reject all" button on the first layer.

- Fine: €150 million
- Location: European Union and United Kingdom
- Supervisory authority: CNIL
- Legal basis: French Data Protection Act - Article 82, ePrivacy Directive - Article 5(3)
- Case number: SAN-2021-023
- Date: December 1, 2021

5. Conclusion

In today's economy, businesses must attract customers and convince them to consume goods and services to maintain their competitive advantage. With the growth of information technology and the Internet, businesses have easy access to their target audience for advertising and product/service promotion, even intruding into people's

AITBSS
AI and Tech in Behavioral and Social Sciences
E-ISSN: 3041-9433

most private moments. As a result, avoiding the attention economy and business advertisements is almost impossible for most people. In this competitive environment, some businesses will justify using any means, including misleading designs, to convince their target audience to consume more. The connection between fallacies and persuasive technologies can be seen especially in e-commerce websites, where designers attempt to downplay the disadvantages of their products while highlighting their advantages and using logical reasoning to encourage purchases (Lieto & Vernero, 2013).

The use of such tricks can have negative psychological effects on people and become a tool for those with ill intentions to lead them astray. Considering the potential benefits of these tools, it is important to find a solution that can help minimize the risks. Any tool, like a knife, can be used for both good and bad, and there will always be people who are motivated by profit, even if it means engaging in immoral behavior. The responsibility to protect vulnerable groups like children from harmful soft technologies falls on regulators, who must establish rules and regulations in a timely manner to ensure the ethical use of these tools. To ensure the correct use and reduce the risks caused by soft mechanisms, the following suggestions are proposed to improve Iran's laws:

- The law should clearly define the standards for obtaining users' consent for the collection and processing of their personal data. Consent obtained unethically or through dark patterns can undermine Article 59 of the E-Commerce Law and Articles 1–3 of the Computer Crimes Law (Adapted from CNIL French Data Protection Act - Article 82, ePrivacy Directive - Article 5(3), Section 5 of the FTC Act, Spanish Law on Information Society Services - Article 22).
- The statute should specify requirements and procedures for informing users and obtaining renewed consent when storage or research purposes evolve over time or with new applications, thereby strengthening the enforceability of Article 59 (Adapted from Spanish Data Protection Law (LOPDGDD) - Article 11, GDPR - Article 12, 14).
- Privacy limits under normal and heightened security conditions should be clearly delineated to prevent abuse, particularly by government bodies and their affiliates (Adapted from GDPR - Article 5, 7, 12, 14).
- Implementing regulations for the E-Commerce Law should be reviewed and revised; explicitly, Articles 57 and 35 should outline protections for vulnerable groups such as children (Adapted from FTC Children's Online Privacy Protection Act Rule, 15 U.S.C. §§ 6501-6506, GDPR - Article 12(1)).
- The laws should codify clear standards for evaluating and enforcing "the principle of fairness" in the design of websites and software to ensure a minimum quantifiable probability that consumers attain their intended outcomes (Article 46 of the E-Commerce Law can be strengthened and expanded by drawing inspiration from LOPDGDD - Article 6, GDPR - Article 5, the Shanghai Mandatory Compliance Guidelines)
- Increasing punishments proportionate to the crime and defining relative indicators to calculate the cost of punishment that do not require updating the text of the law and create the necessary deterrence (Adapted from GDPR - Article 83, Dutch Policy Rules Administrative Fines 2019).
- Institutional monitoring of compliance with legal requirements to protect consumers against dark patterns as a standard. For example, just as the amount of pollutants used in car pads is not detectable to the average consumer and monitoring compliance with legal requirements can be achieved by a regulatory body and its expert testing, dark patterns are also not easily detectable by the general public. (Expanding the subject of Article 48 of the E-Commerce Law from focusing on goods and services received by consumers in cyberspace to dark patterns imposed on consumers, inspired by GDPR - Article 58)
- The e-commerce law approved in 2004 should be revised and strengthened, as it will be an important part of any future data protection legislation in Iran.
- Future studies should conduct more in-depth research into data ownership and protection, with the aim of utilizing these findings to inform the revision of related plans and bills. Additionally, examining the experiences of countries such as Japan or developing Muslim countries such as Malaysia, Singapore, Indonesia, Turkey, etc. can be valuable in developing effective data protection strategies in Iran.

AITBSS AI and Tech in Behavioral and Social Sciences
E-ISSN: 3041-9433

Ultimately, Iran should enact laws and regulations that restrict and prohibit the use of dark patterns and deceptive soft technologies, particularly in e-commerce businesses, to ensure consumer protection and ethical business practices.

Authors' Contributions

Rasoul Jamshidi: supervision, and validation.
Sattar Rajabpour Sanati: writing-reviewing, and editing.

Declaration

In order to correct and improve the academic writing of our paper, we have used the language model ChatGPT.

Transparency Statement

Data are available for research purposes upon reasonable request to the corresponding author.

Acknowledgments

None.

Declaration of Interest

The authors report no conflict of interest.

Funding

According to the authors, this article has no financial support.

Ethics Considerations

This review article used only published literature, legal documents, and publicly available sources. No human participants, personal data, interviews, or experimental procedures were involved. Therefore, ethics committee approval was not required.

References

Adam, M., Roethke, K., & Benlian, A. (2022). Gamblified digital product offerings: an experimental study of loot box menu designs. *Electronic Markets*, *32*(2), 971-986. https://doi.org/10.1007/s12525-021-00477-0

Banerjee, S., & John, P. (2023). Nudge and Nudging in Public Policy. In M. van Gerven, C. Rothmayr Allison, & K. Schubert (Eds.), *Encyclopedia of Public Policy* (pp. 1-10). Springer International Publishing. https://doi.org/10.1007/978-3-030-90434-0_52-1

Benner, D., Schöbel, S. M., Janson, A., & Leimeister, J. M. (2022). How to achieve ethical persuasive design: A review and theoretical propositions for information systems. *AIS Transactions on Human-Computer Interaction*, *14*(4), 548-577. https://doi.org/10.17705/1thci.00179

Berthon, P., Pitt, L., & Campbell, C. (2019). Addictive de-vices: A public policy analysis of sources and solutions to digital addiction. *Journal of Public Policy & Marketing*, *38*(4), 451-468. https://doi.org/10.1177/0743915619859852

Bombaerts, G., Anderson, J., Dennis, M., Gerola, A., Frank, L., Hannes, T., Hopster, J., Marin, L., & Spahn, A. (2023). Attention as practice: Buddhist ethics responses to persuasive technologies. *Global Philosophy*, *33*(2), 25. https://doi.org/10.1007/s10516-023-09680-4

Brignull, H. (2024). *Deceptive patterns : Exposing the tricks tech companies use to control you*. Testimonium. https://cir.nii.ac.jp/crid/1130862246040860681

Brignull, H., & Darlo, A. (2010). *Dark Patterns.(2010)*. www.deceptive.design

Clavien, C. (2018). Ethics of nudges: A general framework with a focus on shared preference justifications. *Journal of Moral Education*, *47*(3), 366-382. https://doi.org/10.1080/03057240.2017.1408577

de Laat, P. B. (2019). The disciplinary power of predictive algorithms: a Foucauldian perspective. *Ethics and Information Technology*, *21*(4), 319-329. https://doi.org/10.1007/s10676-019-09509-y

Firth, J., Torous, John, Stubbs, Brendon, Firth, Josh A., Steiner, Genevieve Z., Smith, Lee, Alvarez-Jimenez, Mario, Gleeson, John, Vancampfort, Davy, Armitage, Christopher J., Sarris, Jerome. (2019). The "online brain": how the Internet may be changing our cognition. *World Psychiatry*, *18*(2). https://doi.org/10.1002/wps.20617

Fogg, B. J. (2002). Persuasive technology: using computers to change what we think and do. *Ubiquity*, *2002*(December), 2. https://doi.org/10.1145/764008.763957

Gutta, C. (2024). Strengthening Data Privacy Laws in the Age of IoT. *Interdisciplinary Studies in Society, Law, and Politics*, *3*(1), 1-3. https://doi.org/10.61838/kman.isslp.3.1.1

Hagman, W., Andersson, D., Västfjäll, D., & Tinghög, G. (2015). Public views on policies involving nudges. *Review of philosophy and psychology*, *6*, 439-453. https://doi.org/10.1007/s13164-015-0263-2

Hanin, M. L. (2021). Theorizing digital distraction. *Philosophy & Technology*, *34*(2), 395-406. https://doi.org/10.1007/s13347-020-00394-8

Hopster, J. (2021). What are socially disruptive technologies? *Technology in Society*, *67*, 101750. https://doi.org/10.1016/j.techsoc.2021.101750

Iran, I. C. o. (2004a). *Iran's Business Guild Act*. Retrieved from https://rc.majlis.ir/fa/law/show/94011

Iran, I. C. o. (2004b). *Iran's e-Commerce Law*. Retrieved from https://rc.majlis.ir/fa/law/show/93997

Iran, I. C. o. (2009). *Iran's Law of Computer Crimes*. Retrieved from https://rc.majlis.ir/fa/law/show/135717

Kollmer, T., & Eckhardt, A. (2023). Dark Patterns. *Business & Information Systems Engineering*, *65*(2), 201-208. https://doi.org/10.1007/s12599-022-00783-7

Kroll, T., & Stieglitz, S. (2021). Digital nudging and privacy: improving decisions about self-disclosure in social networks. *Behaviour & Information Technology*, *40*(1), 1-19. https://doi.org/10.1080/0144929X.2019.1584644

Kuehnhanss, C. R. (2019). The challenges of behavioural insights for effective policy design. *Policy and Society*, *38*(1), 14-40. https://doi.org/10.1080/14494035.2018.1511188

Lembcke, T.-B., Engelbrecht, N., Brendel, A. B., & Kolbe, L. M. (2019). To Nudge or not to Nudge: Ethical Considerations of Digital nudging based on its Behavioral Economics roots.

AITBSS
E-ISSN: 3041-9433

The 27th European Conference on Information Systems (ECIS),

Lieto, A., & Vernero, F. (2013). Unveiling the link between logical fallacies and web persuasion. Proceedings of the 5th annual acm web science conference,

Luguri, J., & Strahilevitz, L. J. (2021). Shining a light on dark patterns. *Journal of Legal Analysis*, *13*(1), 43-109. https://doi.org/10.1093/jla/laaa006

Macey, J., & Hamari, J. (2024). Gamblification: A definition. *new media & society*, *26*(4), 2046-2065. https://doi.org/10.1177/14614448221083903

Mardiana, S. (2020). Modifying research onion for information systems research. *Solid State Technology*, *63*(4), 5304-5313. https://solidstatetechnology.us/index.php/JSST/article/view/4321

Marin, L. (2021). Sharing (mis) information on social networking sites. An exploration of the norms for distributing content authored by others. *Ethics and Information Technology*, *23*(3), 363-372. https://doi.org/10.1007/s10676-021-09578-y

Nazari, M. (2025). *Endless SMS messages to people/Why don't the promotional SMS messages stop?* Eghtesad-online. https://www.eghtesadonline.com/008dnI

Nouwens, M., Liccardi, I., Veale, M., Karger, D., & Kagal, L. (2020). Dark patterns after the GDPR: Scraping consent pop-ups and demonstrating their influence. Proceedings of the 2020 CHI conference on human factors in computing systems,

Nyström, T., & Stibe, A. (2020). When persuasive technology gets dark? European, mediterranean, and middle eastern conference on information systems,

Özdemir, Ş. (2020). Digital nudges and dark patterns: The angels and the archfiends of digital communication. *Digital Scholarship in the Humanities*, *35*(2), 417-428. https://doi.org/10.1093/llc/fqz014

Pontes, H. M., Schivinski, B., Sindermann, C., Li, M., Becker, B., Zhou, M., & Montag, C. (2021). Measurement and conceptualization of Gaming Disorder according to the World Health Organization framework: The development of the Gaming Disorder Test. *International Journal of Mental Health and Addiction*, *19*, 508-528. https://doi.org/10.1007/s11469-019-00088-z

Rajabpour sanati, S., & Jamshidi, R. (2025). *A Toolbox for Designing Socio-Economic System; A Systems Thinking and Soft Technologies-Based Approach*. Iranian Research Institute for Information Science and Technology (IranDoc). https://irandoc.ac.ir/book/6252

Rajabpour Sanati, S., Jamshidi, R., Rajabi Mashadi, M., & Rangamiz Toosi, A. (2024). Comparing the BAENERGY Mobile App, Iran's Experience with Using Gamification in the Power Grid, with Similar Global Apps. *International Journal of Research and Technology in Electrical Industry*, *3*(2), 410-424. https://doi.org/10.48308/ijrtei.2024.237438.1061

Schmidt, A. T., Engelen, Bart (2020). The ethics of nudging: An overview. *Philosophy compass*, *15*(4), 413. https://doi.org/10.1111/phc3.12658

SharghMediaGroup. (2025). *92% of cybercrimes detected*. SHARGH. https://www.sharghdaily.com/fa/tiny/news-987030

Specker Sullivan, L., & Reiner, P. (2021). Digital wellness and persuasive technologies. *Philosophy & Technology*, *34*(3), 413-424. https://doi.org/10.1007/s13347-019-00376-5

Spiekermann, S., Krasnova, H., Hinz, O., Baumann, A., Benlian, A., Gimpel, H., Heimbach, I., Köster, A., Maedche, A., & Niehaves, B. (2022). Values and ethics in information systems: a state-of-the-art analysis and avenues for future research. *Business & Information Systems Engineering*, *64*(2), 247-264. https://doi.org/10.1007/s12599-021-00734-8

Stieglitz, S., Lattemann, C., Robra-Bissantz, S., Zarnekow, R., & Brockmann, T. (2017). *Gamification*. Springer. https://doi.org/10.1007/978-3-319-45557-0

Sugden, R. (2009). On Nudging: A Review of Nudge: Improving Decisions About Health, Wealth and Happiness by Richard H. Thaler and Cass R. Sunstein. *International Journal of the Economics of Business*, *16*(3), 365-373. https://doi.org/10.1080/13571510903227064

van den Hoven, M. (2021). Nudging for others' sake: An ethical analysis of the legitimacy of nudging healthcare workers to accept influenza immunization. *Bioethics*, *35*(2), 143-150. https://doi.org/10.1111/bioe.12819

Xiao, L. Y. (2022). Blind boxes: opening our eyes to the challenging regulation of gambling-like products and gamblification and unexplained regulatory inaction. *Gaming Law Review*, *26*(5), 255-268. https://doi.org/10.1089/glr2.2022.0012

Zhang, S. (2024). Analysis and Enlightenment of Blind Box Culture" Go Viral". *Journal of Education, Humanities and Social Sciences*, *31*, 101-106. https://doi.org/10.54097/9g02ph93

Zheng, Y. (2024). Buddhist Transformation in the Digital Age: AI (Artificial Intelligence) and Humanistic Buddhism. *Religions*, *15*(1), 79. https://doi.org/10.3390/rel15010079

AITBSS
AI and Tech in Behavioral and Social Sciences
E-ISSN: 3041-9433