IJFANS INTERNATIONAL JOURNAL OF FOOD AND NUTRITIONAL SCIENCES
ISSN PRINT 2319 1775 Online 2320 7876

Research paper UGC CARE Listed (Group -I) Journal Volume 11,Iss 12,Dec 2022

DARK PATTERNS- A STUDY ON THE REGULATION AND EFFECTIVENESS

Mariya Joseph, Assistant Professor, Department of Law, SRM school of Law, Chennai, Tamil Nadu. (mariyaja@srmist.edu.in)

ABSTRACT

Prior to the modern era, all trade and commerce took place physically. After a physical examination and verification, the human epoch felt delight in purchasing anything. The nature and culture of the entire civilization changed as society progressed gradually. Humanity's ultimate goal is to change its appearance, even its colour. E-commerce is completely based on internet. Major transformation in the zone of E-commerce started to take place after the advent of WWW during mid-1990.

The term ‘dark pattern’ was coined by Harry Brignull in 2010. It has become imperative to be watchful and careful in this age of artificial intelligence, where humanity depends on technology for all of its operations. Many businesses use it as payment in exchange for expanding their commercial activities. We offer our own sensitive and important data for the service that is being used. But frequently, people are unaware of the consequences of the information given. Every single service provider adheres to the "Roach model," which is really a ruse that makes it simple to enter but challenging to exit. There are some services and goods that cannot be used without first setting up an account, logging in, or purchasing a subscription. Every online service we use comes with a deceptive design that forces us to buy or use something extra that we did not really mean to. Dark patterns are any interfaces or patterns that pressure users into giving their consent. Any consent gained through coercion, undue influence, or fraud is deemed void, which will have a negative impact on the contract's legalityThis paper analyses about the challenges that dark patterns poses on the economy and the legal regulations and control mechanisms over this.

Key words: E-Commerce, Artificial intelligence, Deceptive design, interface.

ISSN PRINT 2319 1775 Online 2320 7876

Research paper UGC CARE Listed (Group -I) Journal Volume 11,Iss 12,Dec 2022

INTRODUCTION

Prior to the modern era, all trade and commerce took place physically. After a physical examination and verification, the human epoch felt delight in purchasing anything. The nature and culture of the entire civilization changed as society progressed gradually. Humanity's ultimate goal is to change its appearance, even its colour. E-commerce is completely based on internet. E-commerce is defined as "any business transaction concerning goods and services, where participants are not in the same physical location and communicate through electronic means."[1] Another more clear and simple definition of E-commerce is "Any transaction involving goods or services where digital electronic communication performs an essential function."[2] Major transformation in the zone of E-commerce started to take place after the advent of WWW during mid-1990.

The term 'dark pattern' was coined by Harry Brignull in 2010, who defined it as interface designs that "trick users into doing things that they might not want to do, but which benefit the business in question"[3]. The US Federal Trade Commissioner Rohit Chopra also recently defined dark patterns as "design features used to deceive, steer, or manipulate users into behaviour that is profitable for an online service, but often harmful to users or contrary to their intent".[4] It has become imperative to be watchful and careful in this age of artificial intelligence, where humanity depends on technology for all of its operations. Many businesses use it as payment in exchange for expanding their commercial activities. We offer our own sensitive and important data for the service that is being used. But frequently, people are unaware of the consequences of the information given. Every single service provider adheres to the "Roach model," which is really a ruse that makes it simple to enter but challenging to exit. There are some services and goods that cannot be used

[1] Lodder, A and Kaspersen, H (eds), eDirectives: Guide to European Union Law on E-Commerce, 2002, The Hague: Kluwer Law International, p 3

[2] Paul Todd, E-Commerce Law, 2002, p 1.

[3] H, Brignull, Dark Patterns: inside the interfaces designed to trick you, The Verge, available at https://www.theverge.com/2013/8/29/4640308/dark-patterns-inside-the-interfacesdesigned-to-trick-you, last seen on 23/12/2020

[4] Statement of Commissioner Rohit Chopra, Regarding Dark Patterns in the Matter of Age of Learning, Inc. Commission File Number 1723186, 2-9-2020, <https://www.ftc.gov/system/files/documents/public_statements/1579927/172_3086_abcmouse_-_rchopra_statement.pdf>.

without first setting up an account, logging in, or purchasing a subscription. Every online service we use comes with a design that forces us to buy or use something extra that we did not really mean to. Dark patterns are any interfaces or patterns that pressure users into giving their consent. The Indian Contract Act of 1872 makes the idea of free consent very plain[5]. Any consent gained through coercion, undue influence, or fraud is deemed void, which will have a negative impact on the contract's legality. There are many various types of biases being deployed by the companies, which will initially appeal to the audience before becoming a burden. A classic example of a dark pattern is a prompting pop-up message on a website that generates an intention to purchase the product without actually having a need for it.

RESEARCH OBJECTIVES

- To analyse the laws in different countries like USA and UK that regulates dark patterns.
- To identify the challenges faced by the online consumers due to the encroachment of dark patterns.
- To analyse the interplay between DPDP (Digital Personal Data Protection) Bill and dark patterns.

WHAT ARE DARK PATERNS?

A dark pattern is an outcome of the design choice which tricks and manipulates the users into acting in a particular manner while not intentionally choosing that behavior or action. While the waves of academic research[6] into dark patterns identified the phenomena and brought about the typology of the dark patterns, through this section, we map the dark patterns as an outcome of a particular design option opted by the businesses to achieve the manipulation of the end-consumer.

Dark patterns are any such user interfaces intended to coerce a human being's decision-making abilities into choosing something that was actually not their intention. This is a strategy used by

[5] Section 13- it is when two or more persons agree upon the same thing and in the same sense.

[6] Bösch, Christoph, Benjamin Erb, Frank Kargl, Henning Kopp, and Stefan Pfattheicher. n.d. "Tales from the Dark Side: Privacy Dark Strategies and Privacy Dark Patterns." PoPETs Proceedings. Accessed January 9, 2023. https://petsymposium.org/popets/2016/popets-2016-0038.php.; Narayanan, Arvind, Arunesh Mathur, Marshini Chetty, and Mihir Kshirsagar. n.d. "Dark Patterns: Past, Present, and Future | September 2020 | Communications of the ACM." Communications of the ACM. Accessed January 9, 2023. https://cacm.acm.org/magazines/2020/9/246937-dark-patterns/fulltext.; Gray, Colin M., Yubo Kou, Bryan Battles,

various websites and service providers to fool and trap its users. Business ethics are not being used to their fullest potential. Dark patterns are essentially design cues that e-commerce platforms utilise to confuse, mislead, and deceive customers into making unauthorised purchases and disclosing personal information. Dark trends are troubling challenges for businesses and people working in the ecommerce sector. It mainly has to do with deceptive marketing or unethical business tactics utilised by online retailers. In fact, businesses and other organisations that fail to align themselves with data-driven practices risk losing a critical competitive advantage and, ultimately, market share and the accompanying revenue.[7] Importantly, firms have not only the capability of engaging in market manipulation, but also an economic incentive: if some market actors leverage bias, those that do not could be edged out of the market.[8]

The Advertising Standards Council of India (ASCI) announced plans to expand its online advertising policy regarding "dark patterns" earlier in November in an effort to safeguard online shoppers' interests. The group also said that in order to generate more revenue, e-commerce firms spend a significant amount of money designing "black patterns" for their platforms[9]. The European Data Protection Board (EDPB) recently drafted recommendations on the use of dark patterns on social media platforms. Also, it has given designers and users advice on how to look closely at and avoid certain trends on social media platforms that are in violation of GDPR regulations. According to an ASCI estimate, 29% of the advertisements produced in 2021–2022 would involve veiled dark pattern ads that influencers will promote. Among the industries encouraging dark patterns to draw clients are finance, fashion, e-commerce, personal care, and cryptocurrency.

Together with limiting the use of dark patterns, the Center aims to stop false product reviews on e-commerce sites. To prevent phoney reviews on ecommerce platforms, the Indian government recently drafted standards known as "Indian Standard (IS) 19000:2022 'Online Customer Reviews - Principles and Procedures for their Collecting, Moderation and Publishing. To prevent phoney

[7] Hayashi, Alden M. 2013. “Thriving in a Big Data World.” MIT Sloan Management Review. https://sloanreview.mit.edu/article/thriving-in-a-big-data-world/

[8] Hanson, Jon D., and Douglas A. Kysar. n.d. “Taking Behavioralism Seriously: The Problem of Market Manipulation.” NYU Law Review. Accessed January 9, 2023. https://www.nyulawreview.org/issues/volume-74-number-3/taking-behavioralism-seriously-the-problem-of-marketmanipulation/.

[9] https://ascionline.in/images/pdf/dark-patterns.pdf

reviews and to address issues with accessibility and privacy, the new framework requires ecommerce businesses to develop a code of practise and required terms and conditions.

An unsubscribe or opt-out option for unwanted communications or data collection may not be immediately visible to a user. The second technique is "confirmation-shaming," in which the user is "shamed" into complying by framing their decision to reject a particular feature in a certain way. For instance, a user is more likely to accept the offer if they are given the chance to save money when buying an additional product and the choice to decline the same is presented as "No, I do not want to save X amount of money." The third method is "forced continuity," which entails initiating an unnecessary card transaction without providing the customer with a chance to cancel it. This digital snare is designed to prevent users from cancelling their subscriptions. The fourth is "roach motel," which occurs when a user finds it easy to access a particular feature but exceedingly difficult to understand how to depart. A privacy policy that is so complicated that users are dissuaded from opting not to reveal their data is known as a "roach motel," which has a broader definition than forced continuity. Additional examples of deceit include that brought on by recurring commercials, default location sharing settings, and veiled advertisements in surveys. According to Princeton University's empirical investigation, about 1,200 websites contain dark patterns, with roughly 200 of them being blatantly false.

Nearly all user interfaces employ "nudges," which are design elements that influence people's decisions. They are not necessarily unfavourable. Email prompts that alert users when an attachment is missing are examples of positive nudges. Dark patterns, on the other hand, are a more dangerous push since they rely so heavily on deceiving a user into forgoing a particular freedom that they may have otherwise exercised. The need for regulation of these ominous developments to protect private rights resides in this.

While there are various dark patterns within the different business models, in a globalised world, the internet and technological developments have paved the way for the emergence of data-driven business models[10] that value data in economic terms.

[10] 1 Marcinkowski, Bartosz, and Bartlomiej Gawin. 2020. “Emerald.” Data-driven business model development – insights from the facility management industry. https://www.emerald.com/insight/content/doi/10.1108/JFM-08-

Research paper UGC CARE Listed (Group -I) Journal Volume 11,Iss 12,Dec 2022

USA

As was already said, "nudges" need not always be detrimental. Dark patterns, however, are inherently dangerous because they rely on fooling the user into giving up specific information or capabilities. Even more specifically, the recently approved regulation under the CCPA recognises that not all "nudges" may be deceptive dark patterns and only forbids those dark patterns that have "the substantial effect of subverting or impairing a consumer's choice to opt-out" of providing their personal data for the entity's use. A few examples of how the rule might be put into practise include using double negatives like "Don't Not Sell My Personal Information" or making consumers "search or scroll through the text of a privacy policy or similar document or webpage to identify the mechanism for submitting a request to opt-out."

In an effort to standardise compliance, the law even stipulates that businesses must employ a "eye-catching" opt out indicator and a 30-day compliance deadline. Companies are recommended to utilise the logo that is linked in the Attorney General's news release that was previously mentioned. It's interesting to note that the CyLab at Carnegie Mellon University and the School of Information at the University of Michigan compared the suggested icon to existing icon designs. The proposed icon was found to be more effective than others at informing users of their privacy options. The recently enacted California Privacy Rights Act ("CPRA") ballot initiative states that consent granted through a dark pattern is not authorised for the capture of user data and is not informed consent.

The FTC now recognises dark patterns, along with the CCPA and CPRA. ABC Mouse was accused by the FTC of making it difficult for customers to stop paying recurring subscription fees by providing free trials that automatically converted to paid memberships and directing users through a "labyrinth" of pages that compelled them to stay subscribed. The FTC filed a complaint seeking a permanent injunction against ABC Mouse in December 2020. Furthermore, according to the complaint, ABC Mouse uses a "negative option feature," which interprets a user's failure to cancel a subscription as acceptance of the offer. The proposed settlement between Age of Learning and the FTC stipulates that ABC Mouse must provide a simple means for cancelling subscriptions,

2020-0051/full/pdf?title=data-driven-business-model-development-insights-from-the-facility-management-industry.

Research paper UGC CARE Listed (Group -I) Journal Volume 11,Iss 12,Dec 2022

disclose any undesirable options, and get the informed permission of customers. By recommending an additional $10 million punishment, the FTC has made it clear that it intends to continue closely examining the use of dark patterns. FTC pointed out that privacy by design would be one of the principles considered within federal-level data protection law. However, Europe had pioneered the concept of PbD by incorporating it with the GDPR as Data protection by design and default.[11]

Given that the prohibition on dark patterns is dependent on the specifics of each programme and how it affects user choice, law in the USA clearly demonstrates an attempt to find a middle ground between user rights and compliance requirements. Initiatives like The Deceptive Experiences to Online Users Reduction Act (DETOUR Act), which was introduced on April 9, 2019, sought to regulate big web operators by criminalising dark patterns in a more general sense (those with more than 100 million users in a 30 day period). The DETOUR Act would have coupled comprehensive enforcement definitions of dark patterns with important web operators' own self-regulation. Nevertheless, it was never put to a vote by the US Congress. In fact, there have been studies that claim that well under 1% of the users would provide informed onset in such cases.[12]

THE EUROPEAN UNION

Despite the fact that the General Data Protection Regulation (GDPR) does not specifically address dark patterns, it is still against the law to do so without informed consent and without taking organisational and technical steps to ensure privacy by design, which are achieved by incorporating consent management platforms (CMPs). According to a global survey conducted in January 2020 that looked at them after the GDPR went into effect, dark patterns and implied authorization are ubiquitous; only 11.8% fulfil the minimal conditions that we set based on European legislation. The Commission Nationale de l'informatique et des Libertés ("CNIL"), the French data protection body, stressed the need for a framework to govern "dark patterns" by imposing privacy by design and prioritising the user experience over individual choice to ensure that consent is freely given.

[11] 5 https://gdpr-info.eu/art-25-gdpr/

[12] Utz, C., Degeling, M., Fahl, S., Schaub, F., Holz, T. (Un) informed consent: Studying GDPR consent notices in the field. In Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security, 2019, 973–990; https://dl.acm.org/doi/10.1145/3319535.3354212

Research paper UGC CARE Listed (Group -I) Journal Volume 11,Iss 12,Dec 2022

INDIA

Similar to the methods used in the US and the EU, India's planned and existing privacy regulations mainly rely on user agreement and transparency as criteria for protection. The numerous elements that make up "informed" consent, as defined by Section 7 of the Bill, are strongly emphasised in the proposed Digital Personal Data Protection Law, 2022. Prior to collecting a user's personal or sensitive personal data, the Information Technology (Reasonable Security Policies and Procedures and Sensitive Personal Data or Information) Regulations, 2011 (commonly known as the "SPDI Rules"), must get the user's informed consent.

Possibilities for Regulation through the PDP Bill

In order to ensure that user permission is not only informed but also free, explicit, unambiguous, and revocable, the DPDP Bill, 2022, which is based on the GDPR, requires data fiduciaries—entities that control the purposes for which personal data is used—must make comprehensive privacy disclosures. According to theory, practises like opaque privacy policies, the lack of an opt-out option, or pre-checked acceptances of terms and conditions are illegal under the proposed Section 11 of the PDP Bill's consent requirements.

But, as the EU's investigations have demonstrated, significant regulatory action is required to successfully enforce the prohibition on dark patterns. It might not be a good idea to utilise a system that primarily depends on user agreement and openness. This is so that dark patterns, who believe that it suffices to simply alert the user, regardless of how complex their designs may be, can take advantage of the legal loopholes surrounding consent rules and avoid implementing transparency into their designs. Also, a study carried out in the USA found that dark patterns rely on taking use of cognitive biases to give the impression of free permission, which is then defended within a consent-based framework in privacy law.

Thus, the unambiguous ban on dark patterns serves as a crucial motivator to preserve compliance. This is the position taken by the CCPA, CPRA, FTC, and other organisations. In order to address the lack of compliance by multiple companies and websites, the new rule under the CCPA's strategy to restrict the scope of legislation to particular types of dark patterns depending on its

effect on undermining user rights may be an appropriate compromise. This is so because India's privacy laws tend to achieve a compromise between business interests and user rights.

In order to address the shortcomings of a consent-based model of data protection regulation, scholarship in India has also advocated moving away from a solely consent-based approach to data protection. With the consent-based approach, it is the individual's obligation to understand the terms of data sharing. This is not feasible given the vast amount of documents they must analyse and the rising prevalence of algorithmic deductions and automated data collection. It is crucial to grant users unalienable rights over their data and hold the data controller accountable rather than the user in order to ensure that there is a structural shift in the user experience that cannot be undone by merely claiming that the user has been warned.

How laws like the CCPA will be used in practise is still an open question. Indian regulators must first clearly recognise dark patterns within the legal framework in order to prevent informed consent from being compromised by smart interface design, as witnessed in the EU. The JPC must take into account the murky patterns in the most current iteration of the PDP Bill. To accomplish this, the privacy by design architecture must be maintained and its problems must be resolved.

Consumer Protection Law: An Avenue for Regulatory Pluralism

Given the CCPA's past experiences, it is interesting to note that a group of seven significant marketing and advertising trade associations objected to one of the proposed laws in October 2020. The focus of the protests was a plan that would have prevented consumers from having to read or hear a list of reasons why they shouldn't opt out before they could exercise that choice. According to the organisations, the suggested modifications will "unduly hamper consumers' access to factual, vital information regarding the nature of the ad-supported Internet, limiting a consumer's capacity to make an informed decision." But, laws that safeguard consumers might be a step in the right direction. Using underutilised consumer protection laws, this "regulatory pluralism" strategy could be used to fill the gap in privacy laws that do not adequately address manufactured consent, according to academic study. The privacy paradox is when consumers who do care about their privacy are prone to being convinced to act contrary to their own interests. This manufactured

Research paper UGC CARE Listed (Group -I) Journal Volume 11,Iss 12,Dec 2022

consent. According to the same study, the contradiction is more obvious when consumer protection laws are low.

SUGGESTIONS

- To enact proper laws to regulate this unorganized sector.
- To create general awareness among the public.
- To include data that goes outside India in the DPDP Bill, 2022.

CONCLUSION

Dark patterns are vicious technological trap which exerts coercion in the form of mental pressure on the customer. This sector is completely unregulated in India. There should be proper laws enacted as such done in other countries like USA and UK. Without regulating this sector it will be complex to prevent the harmful after effects of this evil practice.