SILICON AND PRECEDENTS

THE LEGAL JOURNAL ON TECHNOLOGY

JOURNAL | **WINTER ISSUE**

VOLUME I - NAVIGATING THE DIGITAL FRONTIER

ISSUE 1

2025

THE LEGAL JOURNAL ON TECHNOLOGY

IN THIS ISSUE

Dark Patterns

AI Judicature

Email Attacks

Gen AI and IPR

Deep Fakes

EDITORIAL BOARD

ADVISORY BOARD

FOREWORD

It has been almost a year since I stepped into my role as Chief Editor of The Legal Journal on Technology. In this time, we have worked hard to pay our debt to the reputation our name carries, transforming what was once a mere blog into a journal of earnest scholarship and practical relevance. My aim, from the outset, was to gather together new voices and seasoned experts, to encourage meaningful debate, and to produce scholarship that can stand firmly in the rapidly evolving tech-legal landscape.

I am delighted to say that we are no longer just an online sounding board—The Legal Journal on Technology has truly come into its own. This new and first Issue reflects the breadth of topics and depth of perspectives we have come to champion:

Dark Patterns and Its Regulation in India: The Genie is Out, Time to Control Him

Opening the volume is an incisive look at manipulative user interface designs —'dark patterns'—whose subtlety masks their power to corrode consumers' autonomy. The author highlights the urgent need for robust regulations, especially as India sharpens its focus on consumer protection in digital spaces.

Nudging Dark Patterns to Light: An Analysis of the Indian Regulatory Landscape with a Comparative Global View

Building on the discussion, this article presents a comparative study, situating India's fledgling guidelines alongside global counterparts. It scrutinizes legislative experiments in Europe, America, South Korea, and beyond, offering a clear roadmap for a more holistic and enforceable regulatory framework on deceptive digital practices.

Exhaustion and Parallel Imports: US vs. EU Perspective

Turning to another frontier—intellectual property—this piece examines how different legal theories of 'exhaustion' play out in transnational trade. By contrasting the United States and the European Union, the author reveals the delicate balancing act between a rightsholder's commercial prerogatives and the competitive demands of open markets.

Beyond Morphing—Unravelling Deep Fake Technology and Its Legal Analysis

The conversation then shifts to deepfake technologies, highlighting the tension between legitimate creative use and their sinister capacity to spread misinformation or cause reputational harm. The article does not merely raise alarms but also sketches out potential legislative routes, thereby aiming to inform and inspire responsible oversight.

AI Judicature: Navigating the Future of Justice

We next explore how artificial intelligence might remold judicial systems—from automating legal research to generating sentencing recommendations. While advocating measured adoption of AI to streamline justice, the paper emphasizes the unyielding importance of procedural fairness, accountability, and judicial prudence.

Distributed Ledger Technology and the Reserve Bank of India

Concluding the Issue is a study on DLT—popularly known through "blockchain"—and its potential to transform financial infrastructures. Focusing on the Reserve Bank of India's exploratory moves, the article suggests that central banks, as the stewards of monetary stability, may well hold the keys to shaping secure, innovative DLT ecosystems in the financial sector.

Collectively, these six articles stand as evidence that our journal is poised to be a serious, thoughtful platform—no longer merely a blog—where the interplay of technology and law is discussed with both depth and practicality. I commend the authors for their meticulous research, willingness to engage with novel dilemmas, and dedication to clarifying some of the most opaque corners of emerging tech.

It is my hope that this Issue and this Journal will add value not just to lawyers and policymakers, but also to technologists, academics, and, indeed, anyone for whom the conversation about fair digital practices and robust legal frameworks matters. We invite debate, dialogue, and further scholarship so that we can remain faithful to our mission: to sharpen understanding and foster progress at the intersection of law and technology.

Enjoy this Issue. Thank you for reading, and for sharing in our ambition to elevate the conversation on how law should adapt—and sometimes lead—in a world where technology's imprint grows more pronounced by the day.

Rudraditya Singh Panwar
Chief Editor
The Legal Journal on Technology

FOUNDER'S NOTE

Founder's Note

Esteemed Colleagues and Readers,

In 2020, recognizing the need to advance a previously underexplored area of law, I founded The Legal Journal on Technology. Our objective was to establish the first inter-NLU law journal, fostering collaboration among National Law Universities and creating a distinguished platform for scholarly discourse at the intersection of law and technology.

Over the past year, our dedicated team has grown to 35 members, each contributing their expertise and unwavering commitment to our mission. We received over 40 submissions for our inaugural issue, encompassing contributions from esteemed professors, dedicated associates, and talented law students alike. After a rigorous selection process, we are proud to present six exceptional articles that set a strong foundation for future publications. These selected works highlight pioneering research and diverse perspectives, underscoring the journal's commitment to excellence and innovation.

In addition to our written publications, we launched a series of podcasts and auxiliary initiatives, strategically designed to complement our academic endeavors and engage a broader audience within the legal community. This multifaceted approach has been instrumental in enhancing our journal's credibility and scholarly impact.

Our transition to a more focused academic approach has solidified our standing as a leading authority in legal technology. By prioritizing rigorous research and high-quality publications, we provide invaluable insights and foster intellectual growth among our contributors and readers.

As we celebrate the completion of our first issue, we are enthusiastic about the future. We are committed to continuing our trajectory of excellence, publishing numerous issues that will explore emerging legal challenges and technological advancements. Our vision is to consistently deliver impactful scholarship that not only informs but also shapes the future of law and technology.

Thank you for your unwavering support and dedication. We look forward to many more editions and the continued growth of our academic community.

Warm regards,

Aryaman
Founder
The Legal Journal on Technology

TABLE OF CONTENTS

Dark Patterns and Its Regulation in India: The Genie is Out, Time to Control Him

YASH DAHIYA

Yash Dahiya is an Advocate practicing in Goa and is an LLM Candidate in International Commercial Arbitration at Stockholm University, Sweden.

Abstract

The use of dark patterns has increased significantly over the years. So much so that it is impossible to ignore its impact on society and hence lawmakers feel the urgency to regulate it. These are deceptive patterns used by websites to induce and manipulate consumers to make decisions that they don't wish to make. The Indian Government last year issued a notification where certain guidelines have been issued to regulate dark patterns in India. 13 dark patterns have been identified under it and thus the author through this paper wishes to analyze the notification. Through this article, the author will explain various dark patterns through websites the author has explored that use such dark patterns. It will enable the readers to understand various types of dark patterns better. The author will also dive into the history of dark patterns and their impact on different laws such as competition law and privacy laws. A look into the international perspective will also be made followed by the possible reservations and the author's personal views. It's high time dark patterns were regulated and the government has taken the right step. Like any other law, changes will be made to the new law based on our experiences.

I. Introduction

Dark patterns have been used for a long time by various commerce platforms all over the world. Harry Brignull introduced the concept of "dark patterns" in 2010, describing it as *deceptive tactics to boost conversion rates.*[1] Before the author goes ahead with this article, it is imperative to define dark patterns. Dark patterns are a user interface designed to trick, persuade, or force a user to make a decision that may not be in their best interests. [2] It serves as a *catch-all term* for a range of actions that compromise the interests of customers to further the interests of the company. [3]

The US Federal Trade Commissioner Rohit Chopra also defined dark patterns as "*design features used to deceive, steer, or manipulate users into behavior that is profitable for an online service, but often*

[1]Spicy IP, 'Dark Patterns Unmasked: Examining Their Influence on Digital Platforms and User Behaviour', (*Spicy IP*, *5* July 2024) <https://spicyip.com/2023/10/dark-patterns-unmasked-examining-their-influence-on-digital-platforms-and-user-behaviour.html#:~:text=Harry%20Brignull%20introduced%20the%20concept,benefiting%20the%20company%20or%20platform > accessed 1 April 2024

[2] *Ibid.*

[3] Arunesh Mathur, Gunes Acar, and others., 'Dark Patterns at Scale: Findings from a Crawl of 11k Shopping Websites' (2019) 3 Proc. ACM Hum Comput. Interact < https://dl.acm.org/doi/10.1145/3359183 >accessed 1 April 2024.

harmful to users or contrary to their intent." [4] The above-given definition could be better explained through an illustration. For example, you are scrolling through the internet and an advertisement pops up of an e-commerce website showcasing heavily discounted products. In that pop, there are two options provided yes or no thanks, I hate saving money. Such tactics are generally to induce consumers by shaming them and thereby making them visit your website and purchase your products. This practice is defined as *confirm shaming.* [5]

Another example is when extra goods or services are added to a shopping cart without the buyer's express consent on the payment page. The consumer has not clicked on donating it but the platform has pre-selected it. The consumer sometimes goes ahead with the purchase, without knowing that it had purchased extra goods or services. This might happen if the consumer thinks the price escalation is due to the taxes, oblivious that the extra price includes additional commodities. Another example is when you want to purchase a fresh pair of shoes you are interested in. You check out the pair of shoes online. But when you discovered it on an online retailer, you saw the message, "Low supply." Purchase now! You almost immediately get this urge to buy the shoes, fearing that if you give it some thought and decide if you really need them or even if you can afford them, it might sell out. [6]

All these examples come under dark pattern practices which are essentially a set of behavioral patterns which aim to puzzle the consumers. The use of dark patterns has considerably grown in India and the rest of the world. [7] Due to such rampant growth, it was deemed pertinent that such practices be regulated. The Central Consumer Protection Authority which is the country's top watchdog for consumers looking at this growth and concern last year issued a notification titled *"The Guidelines for Prevention and Regulation of Dark Patterns 2023"* as a major step to finally regulate such practices. The guidelines have been issued under Section 18 of the Consumer Protection Act 2019. [8] These guidelines have been made taking all the suggestions and comments from the task force set up in June 2023 and various other stakeholders. Before the establishment of the task force, a consultation session was held on June 13, 2023, which was attended by representatives of numerous domestic and international platforms such as Flipkart, Zomato, Google, MakeMyTrip, etc. [9] Through this paper, the author sets out to examine 5 aspects. First is the history and the origin of dark patterns. The second is the psychological element that drives users to get induced by dark patterns. The third is the types of dark pattern practices. The fourth is an examination of foreign regulations covering dark patterns and its impact on different sectors. The fifth are the comments from companies. The sixth are the possible reservations followed by the author's opinion.

Fairtrade practices typically require informed consent, which means users should have a clear understanding of what they are agreeing to when interacting with a website or application. Dark

[4] Rohit Chopra Report Regarding Dark Patterns in the Matter of Age Learning, Inc. Commission File Number 1723186 (Sept 2020).
[5] Linn Ekroth & Josefine Sandqvist, *Confirm shaming and its Effect on Users* (2008) (Unpublished Ph. D. thesis, Jonkoping University).
[6] Ray Sin, Ted Harris, *et. al* (eds.), *Behavioural Public Policy* (Cambridge University Press, Cambridge, 2022).
[7] Manali Palit, 'Protecting Online Consumers: A Deep Dive into Dark Pattern Regulations in India' (2024) 12(2) IJRTI < https://ijcrt.org/papers/IJCRT2402257.pdf> accessed 3 April 2024.
[8] The Guidelines for Prevention and Regulation of Dark Patterns, 2023
[9] Dark Patterns: The New Threat to Consumer Protection (*ASCI,* Nov 2022) < https://www.ascionline.in/wp-content/uploads/2022/11/dark-patterns.pdf> accessed 4 April 2024.

patterns often hide important information or make it difficult to opt out of certain actions, undermining informed consent. [10]

II. History and Origin of Dark Patterns

The term Dark Patterns as reiterated above was laid down by user experience designer Harry Brignull in the year 2010, when he noticed how companies are purposefully creating and embedding patterns into codes to deceive users subtly. He realized that this was an unethical and cunning tactic being used by such companies and thus it was apparent that this needs to be eradicated by creating a code of ethics that companies need to follow. [11] It's kind of like a grey area for the author where companies are indirectly creating a sense of urgency for instance to manipulate the consumers or users. One might argue that the element of choice is still with the consumers but the whole idea of this principle is that you are laying down false facts on the users to induce them which in the author's sense is unlawful. What the author of this paper is trying to say is that the use of psychological strategies is fine, provided they do not cross a certain threshold. For example, the retail industry has a long history of deceptive and manipulative practices that range on a spectrum from normalized to unlawful. Some of these techniques, such as psychological pricing (that is, making the price slightly less than a round number), have become normalized. This is perfectly legal, and consumers have begrudgingly accepted it. More problematic are practices such as false claims of store closings, which are unlawful but rarely the target of enforcement actions. These are marketing tactics aimed at specific consumers that take advantage of their cognitive biases to influence them to make decisions that go against their intended preferences.[12]As time passed, the role of the Internet in daily life increased. Today's online businesses are much more aware of consumers and improve on their marketing tactics by taking advantage of the biases that influence online consumer behavior. When shopping or consuming information online, consumers pay less attention to disclosures, process information less effectively, and more often than not, they rely on basic guidelines when faced with information overload. [13]

Research shows governments started to realize such market strategies and started setting up rules and codes of conduct for such companies to adhere to. They also started setting up dispute redressal mechanisms where the users can bring forward their claims against companies who still adhere to such unscrupulous tactics. Before we dive further into this paper, we must understand the

[10] Rohi Ray, 'Dark Patterns and India's Battle for Ethical E-Commerce' (*University Of Richmond, School of Law,* 4 October 2023) < https://jolt.richmond.edu/2023/10/04/dark-patterns-and-indias-legal-battle-for-ethical-e-commerce/> accessed 5 April 2024.
[11] Harry Brignull, 'Bringing Dark Patterns to Light' (*Medium*, 7 June 2021) <https://harrybr.medium.com/bringing-dark-patterns-to-light-d86f24224ebf> accessed 6 April 2024.
[12] OECD Publishing Report on 'Dark Commercial Patterns (2022).
[13] Jennifer Valentino DeVries, 'How E-Commerce Sites Manipulate You Into Buying Things You May Not Want' (*The New York Times,* 24 June 2019) < https://www.nytimes.com/2019/06/24/technology/e-commerce-dark-patterns-psychology.html > accessed 10 April 2024.
Harry Brignull, 'Bringing Dark Patterns to Light' (*Medium*, 7 June 2021) <https://harrybr.medium.com/bringing-dark-patterns-to-light-d86f24224ebf> accessed 4 July 2024.
OECD Publishing Report on 'Dark Commercial Patterns (2022).

psychosis of the human mind when dealing with dark patterns. What drives a person to make such decisions in haste?

III. Psychological Factor Examination

Consumer behavior encompasses the decision-making processes that both precede and follow the actions that are directly related to obtaining goods or services. Impulsive behavior stems from a constant need to purchase and an incapacity to consider the implications of that purchase. Even with knowledge of the detrimental consequences of purchasing, there's a strong need to meet your most basic needs right away. [14] Burton et al. assert that impulse buying happens when there's a strong emotional desire that strikes out of nowhere and results in reactive behavior with little cognitive control. The instant satisfaction that comes with a purchase helps to explain this propensity to make impulsive, thoughtless purchases. The use of dark patterns and their rise indicates how online platforms have used human psychology as a tool for money-making. [15]

In his book titled *"Thinking Fast and Slow"* David Khaneman suggests that from the standpoint of behavioral science, dark patterns take advantage of cognitive biases like social proof or scarcity bias to get customers to invoke System 1 thinking rather than a more deliberate and thoughtful System 2 thinking. [16] Harry Brignull has laid down that the recipe for dark patterns involves a combination of Applied Psychology, AB Testing, and User Interface Design. [17]

There are however certain studies made as well to mitigate the effect of dark patterns. An experiment was run by Nouwens and his colleagues to comprehend how various dark patterns affect getting users' permission to collect their data. They discovered that the efficacy of various dark patterns varies. The consent rate is unaffected by notification styles (barriers that stop users from interacting until a consent response is received vs. banners that request consent but do not block access) but it is increased by 22–23 percentage points when a "reject all" button is not displayed on the first page. [18]

IV. Categorization of Dark Pattern Practices

Through the instances mentioned above, dark patterns are thus an umbrella term that consists of various types to induce users to perform an action which they know is not good for them.

[14] Rosa Isabel Rodriguez, Paul Lopez and others, 'Factors Affecting Impulse Buying Behaviour of Consumers' (2021) 12 Frontiers in Psychology <https://www.frontiersin.org/journals/psychology/articles/10.3389/fpsyg.2021.697080/full> accessed 4 July 2024.
[15] *Supra* note 14.
[16] Daniel Kahneman, *Thinking Fast and Slow* (Penguin UK 2015).
[17] *Supra* note 11.
[18] Ray Sin, Ted Haris, and others, 'Dark Patterns in Online Shopping: Do They Work and Can Nudges Help Mitigate Impulse Buying?', (2022) Behavioural Public Policy <https://www.cambridge.org/core/journals/behavioural-public-policy/article/dark-patterns-in-online-shopping-do-they-work-and-can-nudges-help-mitigate-impulse-buying/996B92402604A7E3D417ECBAE2C38362> accessed 14 April 2024.

Researchers over the years have attempted to categorize dark patterns in various ways to make understanding and counteract the phenomenon easier. Mathur defined the taxonomy of dark patterns based on analyzing e-commerce websites, identifying seven categories: (1) Sneaking (e.g., hiding information that could have affected users' choice); (2) Urgency (e.g., patterns that place deadlines on the decision); (3) Misdirection (e.g., use of design proprieties to steer users toward a specific choice); (4) Social proof (e.g., the specific choice is driven by the behavior of others); (5) Scarcity (there is limited availability of something, and therefore, its value increases); (6) Obstruction (some choices might be more challenging to make than others) and (7) Forced action (additional action is required to complete a task). [19] Sray, based on the dark patterns identified by Brignull, provided an overview of user experience dark patterns. He categorized patterns into five groups: (1) Nagging (redirection to expected functionality); (2) Obstruction (adding difficulties to the interaction process); (3) Sneaking (hiding information that might be useful, delaying it so it would be disregarded at the decision time); (4) Interface interference (UI design manipulation that emphasizes some aspects over others) and (5) Forced action (user must perform some action to access some functionality). Similarly, Cara focused their review on dark patterns in the context of user experience.[20]

The Guidelines for Prevention and Regulation of Dark Patterns 2023 has identified thirteen such patterns that are being used by various e companies. All platforms that regularly offer goods and services in India, including those from foreign jurisdictions that do so, as well as advertisers and sellers operating in India, will be subject to the guidelines. Additionally, it has categorized dark patterns as unfair trade practices and misleading advertisements, subjecting them to the provisions of the Consumer Protection Act, 2019. [21]

1. **False Urgency** is a tactic used to trick a user into thinking there is a fake sense of urgency or scarcity to get them to act fast and buy something. Usually, the design uses some kind of count, timer, or countdown. This category of dark patterns includes all limited-time offers. These patterns fall into two main categories: either the user has to pay full price until the item they're eyeing is out of stock, or they have a limited time to take advantage of a discount before it expires.[22] The Guidelines for Prevention and Regulation of Dark Patterns 2023 have identified false urgency as a type of dark pattern and have defined it as the following.

"False Urgency" means falsely stating or implying a sense of urgency or scarcity to mislead a user into making an immediate purchase or taking an immediate action, which may lead to a purchase; including:
i. Showing false popularity of a product or service to manipulate user decision;
ii. Stating that quantities of a particular product or service are more limited than they are. *[23]*

---

[19] Arunesh Mathur, Gunes Acar and others, 'Dark Patterns at Scale: Findings from a Crawl of 11k Shopping Websites' (2019) 3(CSCW) Proceedings of the ACM on Human-Computer Interaction 1
< https://dl.acm.org/doi/10.1145/3359183> accessed 16 April 2024.
[20] Nina Gerber, Alina Stover and others, Human Factors in Privacy Research (Springer 2023) 180
[21] Stuti Mazumdar and Simran Bhue, 'Responsible Design Part 4 of 14: False Urgency' (Think Design, April 2022) < https://think.design/blog/responsible-design-part-4-of-14-false-urgency/> accessed 17 April 2024.
[22] Jamie Luguri and Lior Jacob Strahilevitz, 'Shining a Light on Dark Patterns', (2021) 13 (1) The Journal of Legal Analysis 43 < https://www.researchgate.net/publication/350340175_Shining_a_Light_on_Dark_Patterns> accessed 18 April 2024.
[23] *Supra* note 8.

Instances such as there will be pop-ups on the websites when you book a hotel room that says things like "*only 2 rooms left*" or "*100 people are currently browsing this property*." It is a dark pattern when false information is presented to customers in an attempt to instill a false sense of urgency.[24] On having gone across Flipkart, the author found various products that were being sold using the dark pattern of false urgency. (Below is a screenshot of such an instance mentioned in *Figure 1.*)[25]

The author also visited the site Amazon.com where he also encountered such tactics being used. (Screenshot of products being used using false urgency mentioned below in *Figure 2.)*[26]

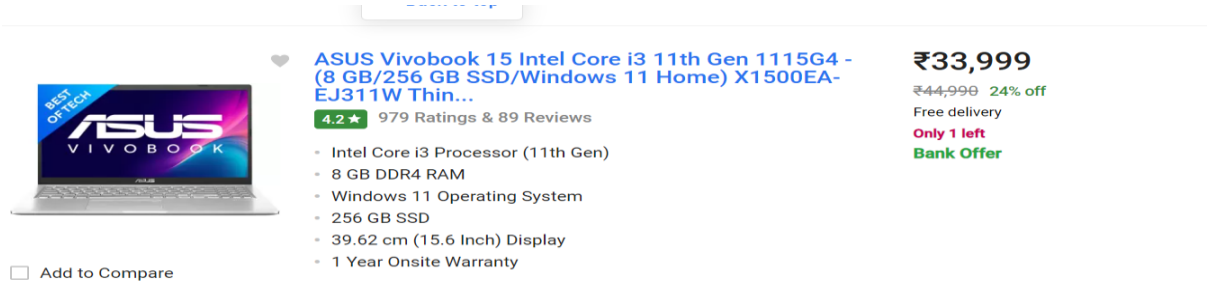

Figure 1. Flipkart.com (Screenshot taken on 19th April 2024 at 1:43 PM)

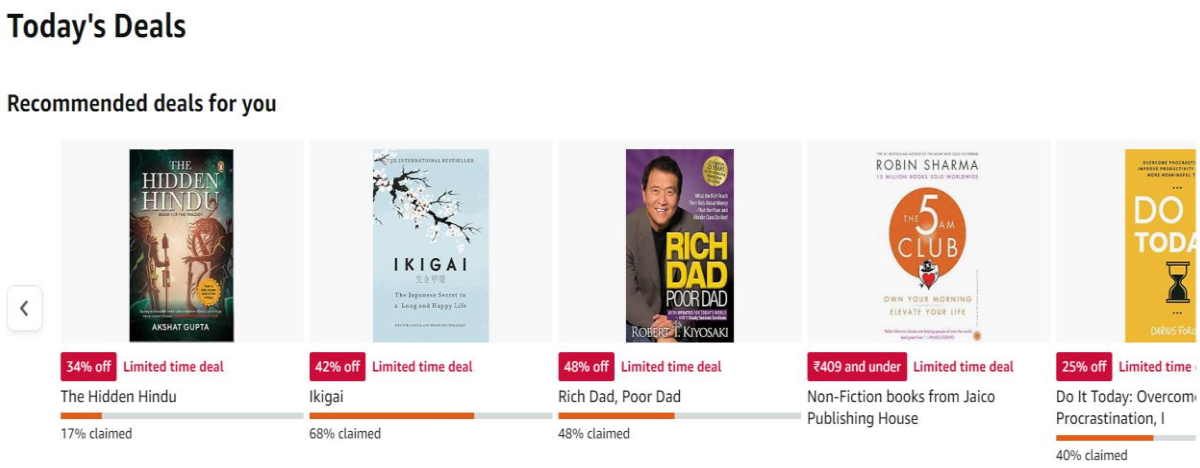

Figure. 2 Amazon.com (Screenshot taken on 20th April 2024 at 1:55 PM)

Thus, the above screenshots are classical examples of how e companies use this method to influence customers and apply pressure on them to make hasty decisions.

2. **Basket Sneaking** is the act of adding extra items—like goods or services, donations, or payments to charities—during a platform's checkout process without the user's express permission. As a result, the total amount due from the user is greater than what was planned for the selected good or service. However, it is pertinent to mention that the addition of free services or any

[24] Sandeep Sharma and Dr. Ishita Sharma, 'Dark Patterns in a Bright World: An Analysis of the Indian Consumer Legal Architecture', (2023) 11 International Journal on Consumer Law and Practice <https://repository.nls.ac.in/cgi/viewcontent.cgi?article=1122&context=ijclp> accessed 20 April 2024.
[25] This is a screenshot taken from the author's computer. Flipkart is one of the most popular e-commerce websites. Here in the screenshot, it is evident that by mentioning only one left, the site wishes to create a false urgency in the minds of the customers.
[26] This is a screenshot taken from the author's computer. Amazon.com is a world-renowned e-commerce website similar to Flipkart. Here you can see that by mentioning the percentage of stock claimed, the site is trying to use the same tactic which can be seen in the above figure.

complimentary services is not considered basket sneaking. [27] On going through Zomato which is a popular food delivery application, in *Figure 3* you can see that on the checkout page, Zomato had automatically added Rs. 2 as a donation to Feeding India in the total. [28]

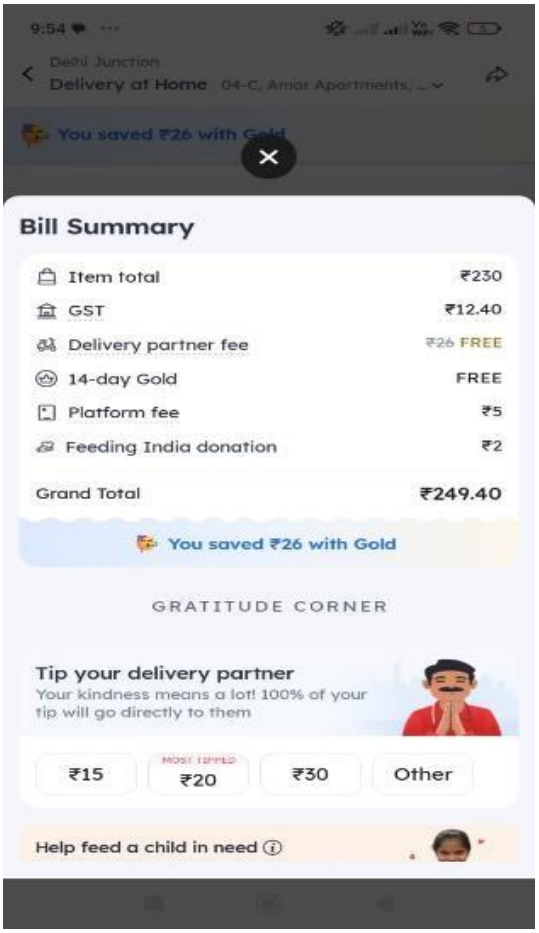

Figure. 3 Zomato.com (Screenshot taken 21st April 2024 at 03: 45 pm)

Similarly, if you go across Blinkit as well, which is also a popular grocery delivery application, you can see that the application has automatically added, Rs. 1 to the total as a donation to Feeding India in *Figure 4*.[29]

[27] *Supra* note 9.
[28] Zomato is a food delivery website operating in India. From the screenshot denoted in Figure 1, it can be seen that the Feeding India donation was added automatically by the platform without seeking permission from the customer. This violates the element of choice and thus is a form of dark pattern which is being employed.
[29] Blinkit also added the Rs. 1 donation without seeking the consent of the consumer and hid it addition in to the total costs.

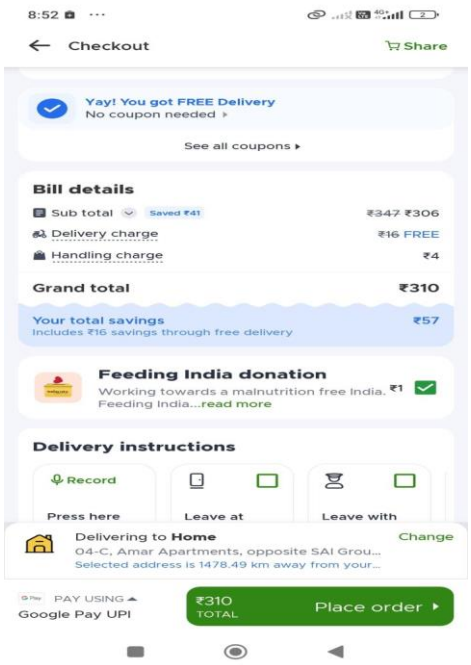

Figure. 4 Blinkit.com (Screenshot taken on 22nd April 2024 at 09:47 am)

While the author does not condemn giving out donations, consumers should have the element of choice whether or not to give additional money or not. It should not be in any sense pre-selected for them.

The whole basis of basket sneaking is based on the premise that consumers usually are quick at the time of checking out and most often do not see the additional expenses that have been added to their total. Most likely consumers assume these additions are merely taxes but this is not true.

In *Figure 5*, you can see that Zomato has added Zomato Gold which has enabled the consumer to avail free delivery and discount. This is not a case of basket sneaking as over here the consumer is being benefited and there is no inducement involved.

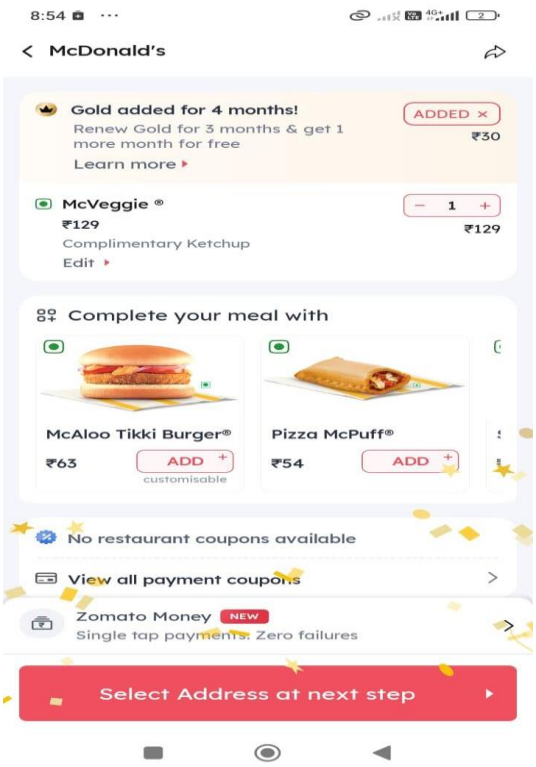

Figure. 5 Zomato.com (Screenshot taken on 25th April 2024 at 11: 13 am)

3. **Forced Action** involves forcing consumers into taking an action they may not want to take, such as signing up for a service to access content. [30] For instance, a health and wellness website forces users to subscribe to their monthly newsletter to purchase their products. The guidelines on dark patterns have defined forced action as

"forcing a user into taking an action that would require the user to buy any additional goods or subscribe or sign up for an unrelated service or share personal information to buy or subscribe to the product or service originally intended by the user." [31]

The guidelines also lay down various illustrations of forced actions some of them include

"a. prohibiting a user from continuing with the use of product or service for the consideration originally paid and contracted for, unless they upgrade for a higher rate or fees;

(b) forcing a user to subscribe to a newsletter to purchase a product;

(c) forcing a user to download an unintended or unrelated separate app to access a service originally advertised on another app e.g. A user downloads app, X, meant for listing houses for renting. Once the user downloads X, they are forced to download another app, Y, for hiring a painter. Without downloading Y, the user is unable to access any services on X;" [32]

---

[30] Department of Consumer Affairs Urges Online Platforms to Refrain from Adopting 'Dark Patterns' Harming Consumer Interest (*Press Information Bureau*, 30 June 2023) https://www.pib.gov.in/PressReleseDetailm.aspx?PRID=1936432 accessed 26 April 2024.
[31] Tanmay Songade, 'Prevention and Regulation of 13 Dark Patterns in India' (*Medium* 9 Jan 2024) <https://medium.com/@tanmaysongade/prevention-and-regulation-of-13-dark-patterns-in-india-7d9a4eee278a> accessed 26 April 2024.
[32] *Supra* note 8.

In going through the website of Byjus, it is seen that the company does practice forced action by forcing customers to enter their phone numbers if they want to access their course materials. (Screenshot of the website attached below *Figure 6*.) After entering your phone number and verifying it by OTP, you are subject to calls from the company trying to advertise their offers. [33] Forced action instruments of dark patterns have been growing significantly in the UPI industry as it has grown significantly in the past decade. A national survey conducted by LocalCircles found out that although UPI transactions are meant to be free, 41% of respondents said they had encountered the "forced action" method, in which they were required to give their contact list to use the wallet payment service, or had their funds in the online wallet blocked up to a certain amount. [34]

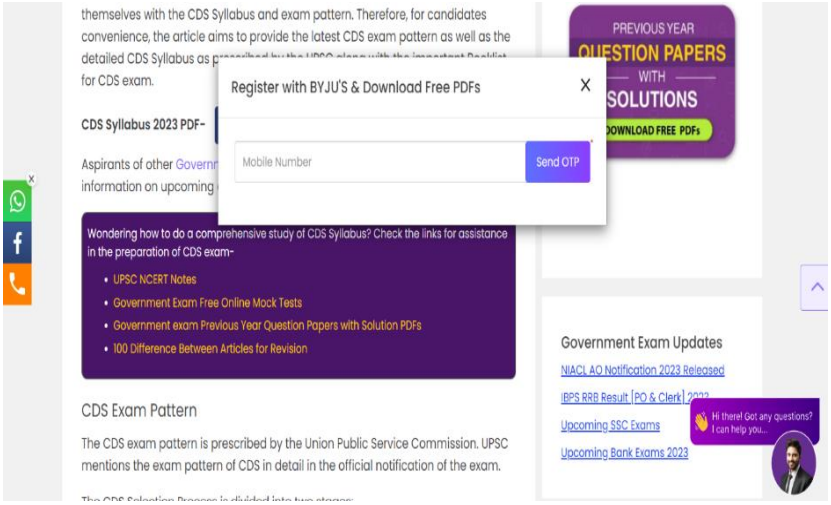

Figure. 6 Byjus.com (Screenshot taken on 27th April 2024 at 09:57 am)

4. **Subscription trap** also known as the roach model. As the name implies, subscription trapping is the deliberate process of making it difficult, drawn-out, and unclear to cancel a paid subscription (e.g., by concealing the cancellation option or creating complicated cancellation). [35]

Therefore, it is imperative to guarantee that the cancellation process is uncomplicated, transparent, and clear for subscriptions. Furthermore, extraneous information or steps, like requesting payment details or enabling auto debit instructions, should not be necessary when it comes to "free subscriptions."[36] When going through the popular online chess platform Chess.com, it can be seen

[33] Byjus is an e-learning platform providing highly adaptive, engaging, and effective learning solutions to more than 150 million students around the world.
[34] 1 in 2 consumers surveyed confirm experiencing one or more dark patterns with online payment platforms: Hidden Charges, Forced Action, Subscription Trap along with Bait and Switch often experienced by consumers (Local Circles 10 April 2024) < https://www.localcircles.com/a/press/page/hidden-charges-payment-platforms > accessed 27 April 2024.
[35] Ashley Sheil, Gunes Acar, and others, 'Staying at the Roach Motel: Cross Country Analysis of Manipulative Subscription and Cancellation Flows', (CHI Conference on Human Factors in Computing Systems, Houston. 11 May 2024) < https://dl.acm.org/doi/10.1145/3613904.3642881 > accessed 28 April 2024.
[36] *Supra* note 8.

that to avail of the free trial of the features of the site, the user has to insert card details that do not make sense. (Screenshot of the website attached below as *Figure 7 & 8*). [37]

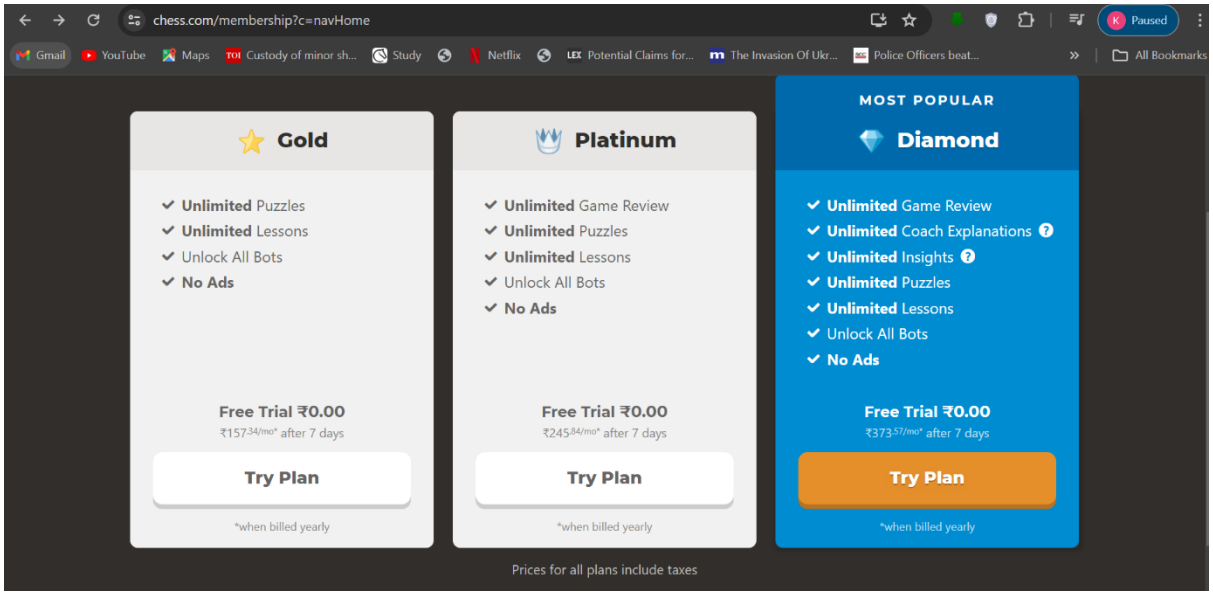

Figure. 7 Chess.com (Screenshot taken on 28th April 2024 at 02:15 pm)

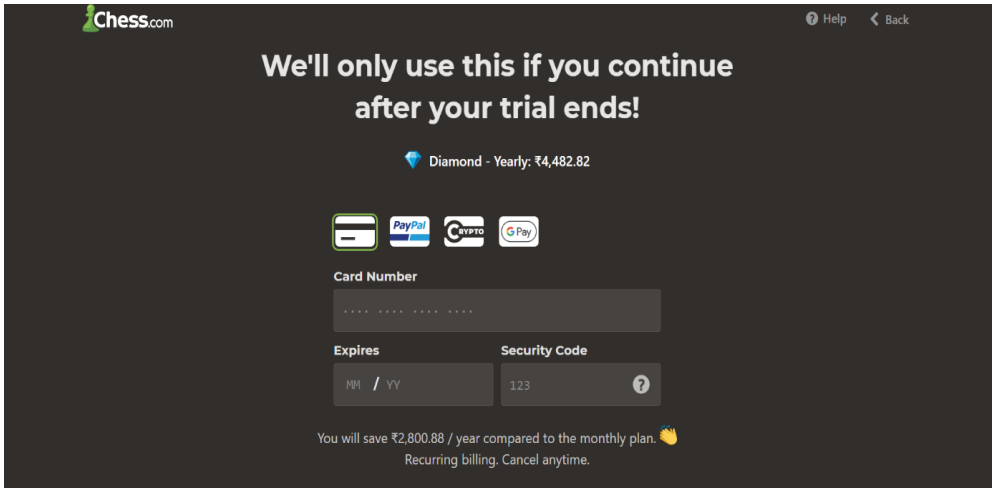

Figure. 8 Chess.com (Screenshot taken on 30th April 2024 at 09:15 am)

5. **Interface Interference** refers to the way a website or app's design tricks users into doing things they don't want to do by emphasizing some information while concealing other important details. [38] For example, hiding the cancel button in a tiny font or providing a light-colored "No" option when a pop-up window asks for a purchase. Another trick might be to click the 'X' icon to close a pop-up window that opens another advertisement. In essence, it's about designing user interfaces that deceive people into doing things they shouldn't. [39] If you go across the site SSBCrack.com, you

[37] Chess.com is an online chess-playing website where users can play chess amongst themselves online.
[38] *Supra* note 8.
[39] *Supra* note 22.

can see how interface inference is being employed by them. (Screenshot of the website attached below as *Figures 9 and 10*) [40]

Figure 9. SSBCrack.com Books being sold (Screenshot taken on 1st May 2024 at 5:45 am)

In *Figure 9*, books of SSB Crack are being sold on the website on the side. However, when the author tried to click the cancel button, it automatically took the author to the Amazon website from which he could buy the book. Despite, repeated cancellation attempts, it always took him author to the Amazon website. Refer to *Figure 10*.

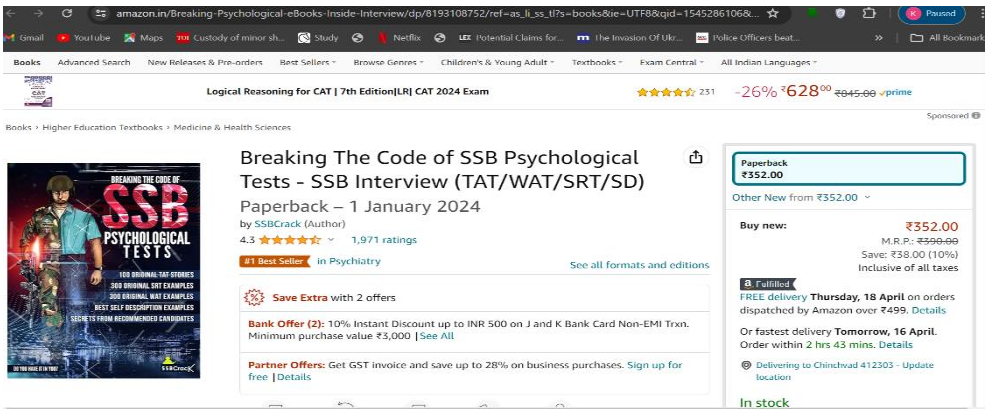

Figure 10. Amazon.com (Book shown in Amazon) (Screenshot taken on 2nd May 2024 at 5:50 am)

On exploring the popular language learning site, Duolingo, by the responders on a survey conducted by the Internet Freedom Foundation, it was found that the app has advertising for free users. There is a mute button that keeps moving around and is blended with the advertisement that make users unable to mute the ad. [41]

6. **Bait and Switch** is advertising a particular outcome based on the user's action but deceptively serving an alternate outcome. Customers are tricked into using a product under alluring terms, and then once engaged, the terms are changed to force them to accept the result, which is typically a

[40] SSBCrack.com is an e-learning platform that shares study resources with students who are planning to try for the defense forces. They prepare you for various defense exams.
[41] Duolingo is an American education technology platform that provides various language learning courses such as Spanish, Italian, Mandarin, etc to its users.

paid service. For example, A "Free Version" button may be prominently displayed on a software download page, but upon installation, the programme only offers a trial period and requests payment. [42]

Another instance is when you search for a travel price and in the search results you see a reasonable price. However, when you click on it further, you see a completely different price than the one mentioned. (Like in the below image (*Figure 11*). [43]

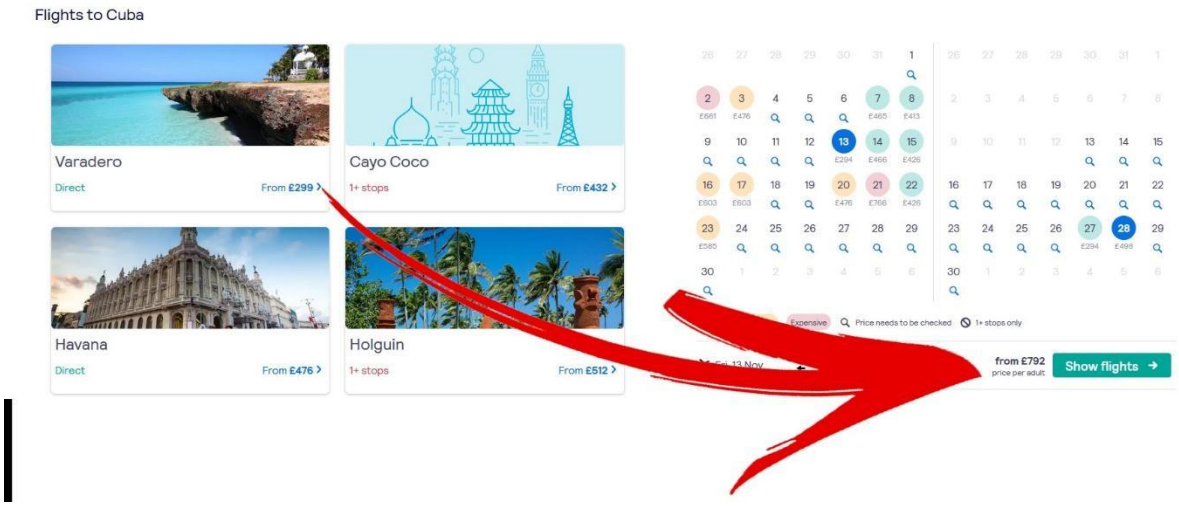

Figure 11 (Image taken from Investopedia.com where it was discussed)

7. **Drip Pricing** is a practice where potential customers are only given access to a portion of a product's price, such as taxes, which are costs that nearly all consumers must pay. As a result, the entire cost is only disclosed very recently during the purchasing process, which raises questions about the final cost and makes it difficult to compare prices. Therefore, it could be said that these kinds of representations are deceptive. All or most applicable non-optional taxes, duties, fees, and charges must be included in the quoted prices.[44] It hinders the consumer's ability to compare prices and make an informed decision. Research conducted by the Dept of Business and Trade (United Kingdom) found that out of the 525 online and mobile app providers in their sample, 46% charge at least one drip fee during the checkout process (which does not include delivery fees).[45]

8. **Disguised Advertisement** is any advertisement that resembles editorial or naturally occurring content and needs to make it obvious that it is an advertisement. Influencer posts, sponsored reviews, and advertisements styled to look like content are a few examples.[46]

For instance, ongoing across a blog published by Enhelion titled *"Regulation of Cross Border Mergers and Acquisitions in India, UK, and USA"* you can see that at the end, Enhelion has advertised its

[42] *Supra* note 9.
[43] *Ibid.*
[44] David Muir, Katja Seim, and Anr, 'Drip Pricing When Consumers Have Limited Foresight: Evidence from Driving School Fees', (2023) SSRN Electronic Journal <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2220986> accessed 3 May 2024.
[45] Department of Business and Trade, *Estimating the Prevalence and Impact of Online Drip Pricing*, (2023)
[46] Sarah Cornwell and Victoria Ruben, 'Native Advertising: Ads in Disguise as Editorials' (2018) Proceedings of the Annual Conference of CAIS <https://www.researchgate.net/publication/335048542_Native_Adverstising_Ads_in_Disguise_as_Editorials> accessed 3 May 2024.

master's course in Corporate Laws which brings doubt as if the whole blog was published for the reason of advertising its course. (Screenshot of the website attached below as *Figure 12.)* [47]

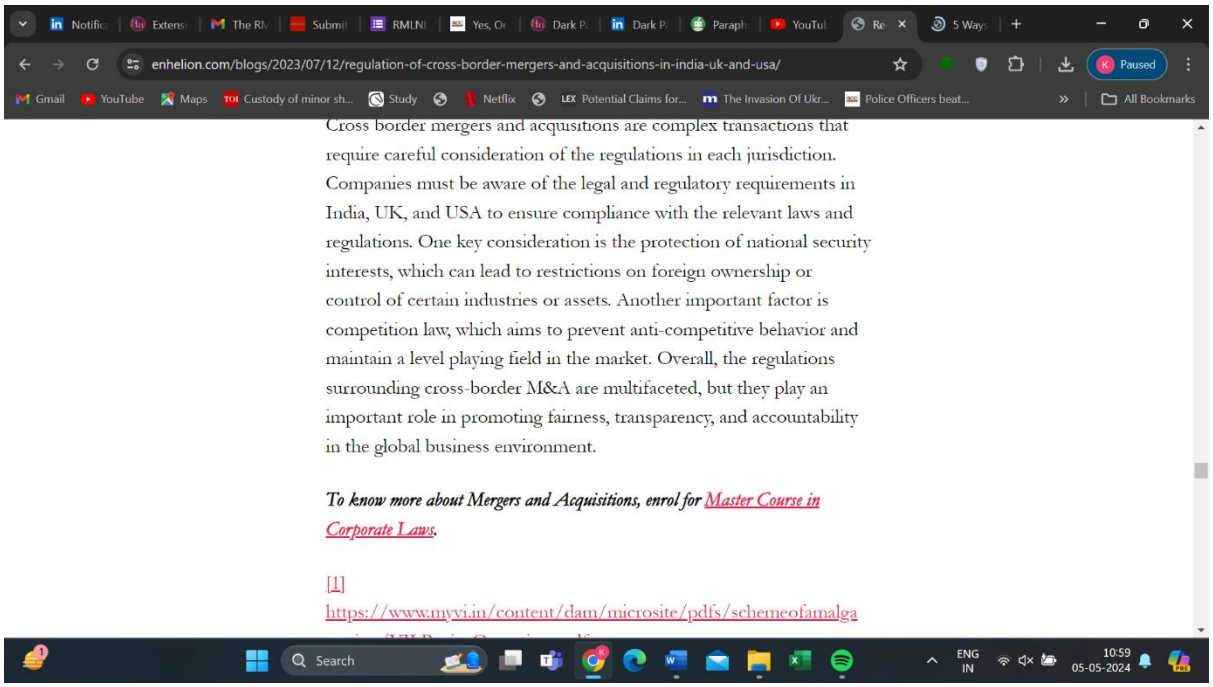

Figure. 12 Enhelion.com (Screenshot taken on 17th May 2024 at 8:15 am)

9. **Nagging** is a type of dark pattern in which a user is disrupted and annoyed by repeated and persistent interactions, in the form of requests, information, options, or interruptions, to effectuate a transaction and make some commercial gains, unless specifically permitted by the user.

For instance, in 2018, Instagram repeatedly and relentlessly pestered users to enable notifications for several months. The only way for users to refuse the request was to select "Not Now," which kept them from rejecting it completely and letting the nagging continue. (Screenshot of the site attached below as *Figure 13*). [48]

A responder commented on the report published by Internet Freedom Foundation, that

"Hathway has been spam calling for the past 7 months to get a new connection after I disconnected it. I have requested them to stop calling me several times but they don't listen and continue calling me to this day at odd hours."

[47] Enhelion.com is an online platform that provides law online courses at cost-friendly prices. The courses have been drafted and taught by certified professional lawyers.
[48] Instagram.com is a social media platform owned by Meta. It is a photo and video-sharing social networking service.

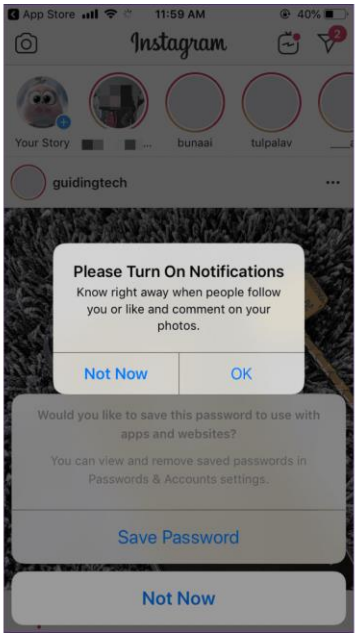

Figure. 13 Instagram.com (Screenshot taken on 18th May 2024 at 10:10 am)

10. **Trick Question** is a dark pattern, in which the user is misled into taking an action, due to the presentation of confusing or misleading language. It takes advantage of ambiguous language to mislead and deceive users. Users often do a fast reading when they are presented with a sheer volume of information. This means that they don't focus on every word on every page. Trick wording usually takes advantage of the scan reading strategy, by making a piece of content look like it's saying one thing but it is asking something which is not in the user's interest.[49]

11. **Rogue Malware**: This dark pattern may be used to obtain consent for processing a customer's data by way of their purchase of the anti-malware tool or software. It is also known as scareware or ransomware and is designed to deceive users into thinking their computer is infected with a virus to get them to pay for a phony malware removal tool that installs malware on their system. It may also include pirated platforms but they get pop-ups that contain malware-infected advertisements. Moreover, users may be directed to an advertisement by default or compelled to click on it, at which point they may find that their private files have been locked and that they must pay to unlock them.

12. **Saas Billing:** refers to the process of creating and receiving payments from users on a recurrent basis. This is achieved by taking advantage of positive acquisition loops in recurring subscriptions to obtain money from customers. For example, in order to get access to exclusive content, a user registers for a free trial on an OTT platform. They are not made aware that their free trial will automatically turn into a paid subscription after a predetermined amount of time throughout the enrollment procedure. Because of this, the user gets unexpectedly charged for the membership once the trial expires without being notified or reminded beforehand. [50]

---

[49] Dark Patterns in Data Protection, (*Licks Attorney's Compliance Blog*, 8 May 2023) < https://www.lickslegal.com/post/dark-patterns-in-data-protection> accessed 19 May 2024

[50] Dipak Rao, 'Dark Patterns in India' (*Singhania and Partners*, 18 April 2024) < https://singhania.in/blog/dark-patterns-in-india> accessed 25 May 2024.

13. **Confirm Shaming:** According to Harry Brignull, a UX consultant based in the United Kingdom, the term " *confirm shaming*" refers to "*the act of guilting the user into opting into something*." [51] The language around the decline choice is designed to intimidate the user into complying. In order to illustrate shaming, the document uses the statement "*I will stay unsecured*" in response to declining to purchase insurance.

There is a deep interrelationship between dark patterns and connections with digital protection, consumer rights, and competition law. The subsequent parts will look into the impact of dark patterns on different sectors.

V. Dark Patterns and Its Impact on Digital Protection

Privacy is an innate desire of humans that has been apparent throughout history. Alen Westin defines privacy as *"the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others".*[52] A person's free consent is implicitly violated when dark patterns are used to deceive customers. Dark patterns are frequently used to obtain a great deal of user data by asking a person for information that is not required for a specific transaction. Third parties are additionally provided access to the gathered data and user profiles. By merging it into the transactional process, consent is obtained for the same.[53] Luiza Jarovsky who is the CEO of Implement Privacy says that

"When a company launches a privacy-invasive device or software, e.g., one that collects or processes data unexpectedly or that unnoticeably surveils passersby or third parties, it bypasses autonomy through architecture. So our autonomy - one of the most central aspects of being human - is being threatened, a perspective which I do not see being sufficiently handled."[54]

Professor Woodrow Hartzog, professor of law and computer science at Northeastern University, argues that in his book "***Privacy Blueprint***" the way user interfaces are designed plays a key role in eroding a user's privacy. He writes privacy laws need to take into consideration how big of a role design plays in privacy, noting privacy laws should "*be careful to broach design in a way that is flexible and not unduly constraining*" while also setting "*boundaries and goals for technological design*." [55]

Dark patterns incorporate nudges which are design choices that are present on almost all interfaces and affect people's decisions. These aren't always bad things. There are positive nudges for example which include things like email prompts that notify users when an attachment is missing. But because dark patterns inherently rely on tricking a user into giving up a certain free choice that they could have otherwise exercised, there are a more problematic kind of nudge. Not all online choice architectures that violate the ability of consumers to make autonomous and informed choices should be considered dark patterns. [56] Online service providers have become increasingly

---

[51] *Ibid.*
[52] Alan F. Westin, Privacy and Freedom, (New York: Atheneum, 1967).
[53] *Supra* note 22.
[54] Agnieszka Kitkowska, Human Factors in Privacy Research (Germany; Springer, 2022)
[55] Woodrow Hartzog, *Privacy's Blueprint- The Battle to Control the Design of New Technologies* (Harvard University Press (2018)
[56] *Supra* note 18.

sophisticated in deceiving users by resorting to a bundle of privacy-dark strategies. This includes strategies such as excessive data collection and storage, denying data subjects control over their data, making it hard or even impossible for data subjects to learn how their data is collected, stored, and processed, etc. Thus, causing grave privacy harm to the users. Thus, it becomes necessary that dark patterns are regulated to safeguard people's right to privacy.

There have been attempts to classify dark patterns concerning privacy as well. Bosch reviewed dark privacy strategies and dark patterns in his research and had proposed 8 dark patterns in his paper. [57] The Norwegian Consumer Council which is a consumer group that is active in the field of digital rights published a report in 2022 where they explained how tech companies such as Facebook, Google, and Microsoft are using dark patterns and default settings to nudge users towards privacy intrusive options. The intention was not to categorize dark patterns but through the report, the following six such design techniques have been identified among the analyzed software: (1) Privacy-intrusive default settings; (2) Unequal ease (the number of clicks) for privacy-friendly options; (3) Visual design (color and symbols) that leads toward intrusive privacy option; (4) Language that leads toward intrusive privacy option; (5) Privacy unfriendly option presented without "warnings"; (6) Users cannot postpone the decision while accessing the service in the meantime.

The General Data Protection Regulation (GDPR) mandates that services be designed with data protection by default and by design, and it also requires businesses to use user data only for legitimate purposes. Dark patterns are not explicitly mentioned in the GDPR. However, in the Norwegian Consumer Council report such companies are running contrary to these regulations by using dark patterns to mislead users to "choose" invasive instead of data protection-friendly options. [58] An international study looking at dark patterns in January 2020 discovered a dearth of enforcement in this area, concluding that "*dark patterns and implied consent are ubiquitous; only 11.8% meet the minimal requirements that we set based on European law." [59]*

Noticing the development of dark patterns, Commissioner for Justice and Consumer Protection of the European Union, Didier Reynders, announced on December 9, 2022, that the European Commission would focus its efforts in 2023 on the regulation of dark patterns and their relationship to the GDPR, as well as transparency in the online advertising market.[60] Subsequently, in February 2023, the European Data Protection Board (EDPB) published guidelines explaining how to recognize and avoid dark patterns. The document offers convenient advice to providers, managers, social media designers, and users regarding how to behave with these interfaces that violate GDPR privacy. [61]

In the United States of America, to reduce the use of dark patterns, several states have put their laws into effect. At the moment, dark patterns are specifically mentioned in three out of five US state

[57] *Supra* note 54.
[58] Forbrukerradet Report on Deceived by Design (2018).
[59] Midas Nouwens, Illaria Liccardi and others, 'Dark Patterns after the GDPR: Scrapping Consent Pop-Ups and Demonstrating their Influence' (2020) 20 (CHCS) Proceedings of the 2020 CHI Conference on Human Factors in Computing System 1 < https://dl.acm.org/doi/proceedings/10.1145/3313831> accessed 30 May 2024.

[60] Dan Cooper, Sam Jungyun Choi and other, 'The EU Stance on Dark Patterns' (*Covington*, 31 January 2023) < https://www.insideprivacy.com/eu-data-protection/the-eu-stance-on-dark patterns/#:~:text=On%20December%209%2C%202022%2C%20the,advertising%20market%20and%20cookie%20fatigue > accessed 2 June 2024.
[61] European Data Protection Board's Guidelines 3/2022 on Dark Patterns in Social Media Platform Interfaces: How to Recognize and Avoid Them

privacy laws. Agreements obtained through dark patterns are not included in the definition of valid consent under the California Privacy Rights Act (CPRA), Colorado Privacy Act (CPA), and Connecticut Data Privacy Act. There are harsh consequences for breaking these rules. The severe consequences that businesses face for disobeying consumer protection laws are highlighted by these penalties, which can reach up to $7,500 per violation in California, $5,000 in Connecticut, and $20,000 in Colorado. [62]

India needs to analyze the approaches made in the European Union and the USA and effectively regulate privacy concerns concerning dark patterns. There are certain shortcomings concerning the new consumer notification which the Author will deal with separately ahead.

VI. Dark Patterns and Its Impact on Competition Law

Owing to their vast user bases and platform roles, online stores like Amazon and operating systems like Android are crucial to the digital economy as a whole. However, there are legitimate anti-trust concerns as these big companies such as Google, Amazon, Meta, etc, acquire greater access to big data, which they can then sell to marketers to boost their presence in online markets. These dominant companies can use manipulative techniques such as dark patterns and such actions have the exclusionary effect in addition to being unfair and exploitative. They make it extremely difficult for new businesses to enter the market because they can't be expected to compete with well-established businesses that have access to massive amounts of big data. The dominant companies can strengthen their market share by using the data to target advertising. [63] In several instances, the Competition Commission of India has noted that data is a crucial non-price competition factor in the online market. As a result, it ought to look into whether these companies have abused their market dominance by violating user privacy. [64]

Under the competition law, coercion is a key component of the abuse of market dominance and has been regarded as an exploitative practice. [65] The Competition Commission of India ordered an investigation into WhatsApp's then-proposed privacy update in 2020, forcing users to either opt out of WhatsApp completely or share even personal data that is not necessary for using the messaging and call services. Given that WhatsApp was determined to be a dominant player in the relevant market and that users would be compelled to accept these terms, the Commission

---

[62] Amy Lee Tan, 'Illuminating Dark Patterns: US Regulators Crack Down on Deceptive Practices Targeting Consumers' (*Science and Technology Law Review*, 17 February 2024) < https://journals.library.columbia.edu/index.php/stlr/blog/view/593#:~:text=Currently%2C%20three%20of%20five%20US,the%20definition%20of%20valid%20consent.> accessed 5 June 2024.

[63] Information Commissioner's Office and the Competition and Markets Authority Consultation paper on Harmful Design in Digital Markets < https://www.drcf.org.uk/__data/assets/pdf_file/0024/266226/Harmful-Design-in-Digital-Markets-ICO-CMA-joint-position-paper.pdf> accessed 13 June 2024

[64] Reuben Philip Abraham and Afif Khan, 'The Jurisdictional Conundrum in Competition Commission of India's Investigation against Whatsapp' (*Kluwer Competition Law Blog*, 18 June 2021) < https://competitionlawblog.kluwercompetitionlaw.com/2021/06/18/the-jurisdictional-conundrum-in-competition-commission-of-indias-investigation-against-whatsapp/> accessed 15 June 2024.

[65] Kajal Dhiman, 'Abuse of Dominant Position Under Competition Act, 2022' (*Manupatra*, 20 June 2022) < https://articles.manupatra.com/article-details/ABUSE-OF-DOMINANT-POSITION-UNDER-> accessed 20 June 2024.

determined that WhatsApp had a prima facie case of abuse of dominance. In 2020, the Commission determined that Google had abused its market dominance when it restricted payments on its Play Store to GPay. [66] Big companies are often incorporating dark patterns on their websites and hence are stealing data which they use to get unfair advantage over their competitors. Thus, dark patterns have an impact over competition law as well.

Another angle is the walled garden approach. Walled garden approach is a closed platform or ecosystem where the platform provider exerts complete control over the content, applications, and media, restricting access according to their preferences. This control aims to establish a monopoly. The walled garden approach is a type of dark pattern that has anti-trust implications. For instance, Amazon's Prime membership caters to various customer needs, offering "Amazon Prime" for binge-watching, "Amazon e-commerce" for shopping, "Amazon Pay" for payments, "Amazon Music" for listening, and connectivity via "Amazon Echo Dot." It can be seen thus that prime membership is a gateway to Amazon's ecosystem, designed to keep customers within its platform, highlighting potential anti-trust concerns. It includes manipulating people's minds to ensure that they don't shop anywhere else thus restricting people. [67]

VII. Comments from Companies Over the Guidelines

The Dark Pattern guidelines even though a noble step are not absolved from shortcomings. While it may be considered a win for consumer protection, businesses, on the other hand, have been critical of the new regulations. A representative of the Asia Internet Coalition (AIC), representing companies like Google, Amazon, Meta, etc said in its comments on the regulations that

"The current formulation of the Draft Dark Pattern Guidelines will increase the regulatory burden on these online, e-commerce, and digital advertising services. These additional regulatory compliances may stagnate the growth of India's digital economy by hurting the ease of doing business." [68] In addition to this, it was requested by the AIC, whether they can self-regulate initially to combat dark patterns. The industry body has stated that, given the dynamic nature of the technological workarounds used to implement dark patterns, self-regulation allows businesses to maintain platform accountability without adding to the burden of compliance by allowing them to periodically update their internal policies. It enables platforms to regulate dark patterns in harmony with the existing laws which include the IT Act of 2000, the Consumer Protection Act, of 2019, and the Digital Personal Data Protection Act (DPDP).[69]

---

[66] *Supra* note 62.
[67] Madhav Tripathi, 'Dark Patterns and Antitrust Laws: Shedding the Light on the Artificial Barriers' (*Centre for Business and Commercial Laws, NLSIU Bhopal*, 15 December 2023) < https://cbcl.nliu.ac.in/competition-law/dark-patterns-and-antitrust-laws-shedding-the-light-on-the-artificial-barriers/ > accessed 1 July 2024.
[68] *Supra* note 9.
[69] *Ibid.*

VIII. Possible Reservations

Though the Dark Patterns Guidelines were introduced with good intentions, their effective implementation is hindered by the lack of suitable provisions. For instance, it makes no mention of the forum to be contacted in the event of a violation of the Dark Pattern Guidelines. The draft had stated that the Consumer Protection Act, 2019 (CPA) provisions would apply in the event of any violation when it was released.[70] However, for some reason, the CCPA did not add this to the guidelines. On the other hand, Annexure 1 states that specified dark patterns practices and illustrations are merely guidance. However, this brings down the enforceability of the guidelines and creates contradiction and confusion. [71] Additionally, by guideline no. 7, in the event of a disagreement or ambiguity, the CCPA's interpretation of the guidelines is considered final. However, since Annexure I is non-binding and only intended to serve as guidance, the CCP has been given the liberty to interpret the dark patterns in newer ways which could lead to confusion at the time of enforcement. It may lead to overbroad interpretation by the CCPA and it lead to discord and even legal action regarding how the CCPA interprets Dark Patterns. [72] As per Guideline No. 4, using dark patterns on any platform is strictly forbidden. Additionally, according to Guideline No. 5, any individual or platform that engages in any of the practices listed in Annexure 1 of the guidelines is considered to be engaging in a dark pattern practice. However, Annexure 1 is non-binding and only serves as a guidance. There is a contradiction between Guideline no. 4 and Guideline no. 5 where Guideline 4 and 5 appear to be directory and Annexure 1 as non-binding. [73]

There is also concern about overlap between existing sectoral regulations and guidelines which can cause uncertainty. For instance, the Insurance and Regulatory Development Authority of India ("IRDAI") prohibits travel portals in India from covertly selling insurance as a default option. The Advertising Standards Council of India ("ASCI"), a self-regulating entity also engaged with drafting the incumbent Guidelines, recently adopted the 'Guidelines for Online Deceptive Design Patterns in Advertising. The Internet Freedom Foundation in its comments on the draft had mentioned this as one of its concerns and the Author agrees with the foundation's possible solution.

"Therefore, we urge the Ministry to be cognisant of regulatory interplay in this domain and delineate its jurisdiction and executive functions from sectoral regulators. While sectoral regulators can undertake suo moto compliance assessment on entities, the Guidelines can act as a public-facing recourse for aggrieved consumers to report dark patterns. Both can coexist harmoniously if jurisdiction is expressly divided at the outset."[74]

---

[70] Akhil Raj and Ekta Gupta, 'Illuminating the Shadows in India's Dark Pattern Guidelines: A Flawed Regulatory Attempt' (*Centre for Business and Commercial Laws*, 20 February 2024) < https://cbcl.nliu.ac.in/contemporary-issues/illuminating-the-shadows-in-indias-dark-pattern-guidelines-a-flawed-regulatory-attempt/> accessed 5 July 2024

[71] *Ibid.*

[72] *Ibid.*

[73] *Ibid.*

[74] Comments on the draft Guidelines on Prevention and Regulation of Dark Patterns, Internet Freedom Foundation <https://content.internetfreedom.in/api/files/divco3ywedt9rpe/vjgsta3321356wn/iff_2023_042_iff_s_comments_on_draft_guidelines_on_dark_patterns_05_10_2023_RC6CGI8oDR.pdf?ref=static.internetfreedom.in> accessed on 1 August 2024.

Another concern is concerning the term "user". The guideline defines a user as, “shall mean any person who accesses or avails any computer resource of a platform.” The Consumer Protection Act, however, does not define the term “user”. It only defines the term “consumer”. It is pertinent to mention that there is a difference between a consumer and a user. It is possible to be a user without buying anything or using any services, but these prerequisites must always be met to qualify as a consumer. The Consumer Protection Act, allows only a consumer to be a complainant in case of a violation and not a user. Thus, unless the Consumer Protection Act incorporates the term user, then despite the existence of the provision regarding the violation of the Dark Patterns Guidelines is assumed in the guidelines itself.

The Dark Patterns Guidelines identify thirteen distinct types of dark patterns, but they also fail to mention some other important and common forms of dark patterns. Other prevalent forms of dark patterns that ASCI identified included "Obscured Pricing," "Privacy Zuckering," "Roach Motel," and "Deliberate Misdirection." Thus, the policymakers did not think it necessary to include these other types of dark patterns in the Dark Patterns Guidelines, even though ASCI itself recognized them. Beyond ASCI, there are additional forms of dark patterns as well such as obstruction, psychological pricing, growth hacking, etc. The Guidelines offer a comprehensive, albeit narrowly defined, list of dark patterns. Therefore, even a small departure from a narrowly defined dark pattern would grant the company a clean sheet. The Guidelines should ideally take a principle-based approach, defining some essential characteristics and outlawing any business practices that fall under them. However, it is also pertinent to mention that the ministry should not prescribe an exhaustive list. [75]

IX. Conclusion and Authors' Suggestions

As reiterated above, the regulations are a welcome step in the Indian framework. In this day and age when users are making every purchase decision based on the kind of deals available and sometimes evaluating the options available can be an overwhelming experience, buyers need a cool-off period to contain their impulses before deciding in haste. The fear of missing out is real and designers need to ensure to not play on this fear through false beliefs.

Dark Patterns spread across different sectors and implicate several sectoral regulators and laws. Sectors like insurance and advertising have their respective legal framework that penalizes the use of dark patterns. For instance, the Insurance Regulatory and Development Authority of India (IRDAI) prohibits travel portals in India from selling insurance as a default option. Competition law also governs 'unfair trade practices', which the dark patterns are characterized as under the Guidelines. It is contended that regarding sectoral regulation, both lines of regulation can exist parallel to each other. Sectoral regulators have the authority to conduct suo moto compliance assessments on entities, and the Guidelines can serve as a public channel for disgruntled customers

[75] *Supra* note 71.

to report suspicious activity. However, it is further contended that the Ministry should be careful not to hinder design and creativity by allowing the imposition of dual penalties. [76]

The Author also contends that there is a vague threshold for penalties. The Guidelines should look at 'the intention to deceive to assess the degree to which the consumer has been harmed and the extent of penalization. Organizations that intentionally harm others by utilizing dark patterns repeatedly or in combination with them may face penalties. Dark patterns also pose a serious threat to the interests of consumers when they collect excessive and unnecessary personal data without the informed consent of the consumers. Since the Digital Personal Data Protection Act of 2023 does not regulate the interfaces or designs used to collect personal data, this risk might still exist after it is put into effect.

The Internet Freedom Foundation has suggested two ways, through which this can be attempted to be regulated.

1. *"The Guidelines could include additional categories of dark patterns that compromise consumer privacy (such as privacy zuckering, nagging, privacy maze, bait and switch, and linguistic dead-ends) and provide illustrations in Annexure 1 to make consumers aware of the data risks associated with them*
2. *The Ministry could suggest standards and principles for platforms or entities engaging in data collection, guiding them on how to minimize the data they collect from consumers and process it transparently. Establishing principles like 'privacy by design', which encourage data protection through inherent technology design, can help meet this objective and mitigate consumer data risks."*[77]

The Author welcomes this as we move to privacy-by-design works in the digital age, "*Privacy by Design*" has become a cornerstone concept for protecting personal data. It was put forth by Dr. Ann Cavoukian and is centered on proactively incorporating privacy considerations into business procedures and IT systems. In the digital age, "*Privacy by Design*" has become a cornerstone concept for protecting personal data, as put forth by Dr. Ann Cavoukian, is centered on proactively incorporating privacy considerations into business procedures and IT systems. [78]

There are several alternatives to dark patterns that a company can incorporate. Large corporations such as Google, YouTube, and Microsoft can integrate moral substitutes for unethical practices on digital platforms. Platforms can offer a retention package in place of Interface Interference, which is simple to sign up for but difficult to unsubscribe from. This will help retain customers. Displaying pop-ups in the left or right corner will help prevent nagging, which is the practice of making repeated, persistent requests for action.[79] Platforms can offer more options as suggestions in place of "basket sneaking," letting customers add relevant products to their carts in case they miss them.

---

[76] *Ibid*.
[77] *Supra* note 71.
[78] Ann Cavoukian, 'Privacy by Design the 7 Foundational' <https://www.ipc.on.ca/wp-content/uploads/resources/7foundationalprinciples.pdf> accessed 10 August 2024.
[79] *Supra* note 1.

Offers and interactions should be clear about the price and main benefits, and privacy deception should be avoided. Businesses can stay away from dark pattern activities and keep customers happy by taking these alternatives into account.

Nudging Dark Patterns To Light: An Analysis Of The Indian Regulatory Landscape With A Comparative Global View

MEDHA CHIRANEWALA

Medha Chiranewala is currently a law student at the Department of Law, University of Calcutta. She is particularly interested in Data Protection, Privacy and concurrent Technology and Cyber Laws.

Abstract

Dark Patterns are designs or user interfaces intentionally crafted to deceive consumers into making choices they wouldn't make. It essentially subverts the choice and autonomy of a consumer availing goods and services online. In light of the increasing usage of such practices in the digital ecosystem, Governments in various jurisdictions have devised laws and guidelines to tackle it, including India. The author in the first section of the article examines the necessity of such safeguards with the help of graphical representations. In the second section of this article, the author examines its applicability to various entities along with different categories of dark patterns and liabilities established under the Guidelines introduced by the Central Consumer Protection Authority (CCPA) of India. In the third section of this article, the author examines and summarizes the laws on dark patterns in various International Jurisdictions such as the EU, USA, Australia, South Korea and Argentina and compares such laws with those of India. In the final section of this article, the author identifies the shortcomings of the Indian legislation and proposes measures to integrate it with other digital laws to make it more comprehensive and enhance Consumer Protection.

I. Introduction

The Central Consumer Protection Authority recently released Guidelines on Prevention and Regulation of Dark Patterns, 2023 in the exercise of powers conferred by section 18 of the Consumer Protection Act, 2019 ("the CP Act") on them. These provisions came into force on 30th November, 2023. This is the first such instance where dark patterns are defined by Indian law, although there already exists a legal framework to deal with unfair trade practices in e-commerce[1]

[1] Consumer Protection Act 2019, s 18.

and misleading and deceptive marketing and advertisements[2]. The guidelines have expanded the ambit of unfair trade practices on e-commerce websites by naming and explaining various tactics or practices which now fall under 'Dark Patterns'.

The term 'Dark Patterns' was first coined by Harry Brignull, a UX Specialist, in 2010, who used it to describe 'deceptive strategies to trick clients'. According to him, *"A Dark Pattern is a manipulative or deceptive trick in software that gets users to complete an action that they would not otherwise have done if they had understood it or had a choice at the time."*[3] The increase in awareness about dark patterns among lawmakers and the general public is what is leading to a trend of implementation of dark pattern regulations in various jurisdictions.

This paper attempts to provide a comprehensive view of the various kinds of dark patterns as outlined by the Indian regulations, the need for such safeguards, the Indian regulatory framework on it, and analysis of such regulations across international jurisdictions such as the European Union (EU), United States of America (USA), Australia, South Korea and Argentina, the comparison between them and the Indian Guidelines and lastly, recommendations for making a robust framework.

II. Why Separate Guidelines? Why Not Unfair Trade Practices?

It is evident that Dark Patterns are unfair trade practices, but the question that arises is - Why is it necessary to have separate laws on Dark Patterns and why aren't the provisions of unfair trade practices enough to address it?

Perusing the Consumer Protection Act 2019 (CP), Section 2(47) defines unfair trade practices as a "trade practice which, to promote the sale, use or supply of any goods or for the provision of any service, adopts any unfair method or unfair or deceptive method..."[4] Which is explained with the help of different instances. While the definition does include 'deceptive methods' against consumers but these methods are limited to the instances given in the provision such as false representation of the goods being of a 'particular standard', 'quality', 'quantity', 'grade composition', 'style' or 'model'; or of the service being of a 'particular standard', 'quality' or 'grade'; or representing that the goods and services have 'sponsorship', 'approval', 'performance', 'characteristics', 'accessories', 'uses' or 'benefits' which they do not have etc.

The reason why this provision falls short of addressing the problem of Dark Patterns is that Dark Patterns, on the face of it, might appear to be legal, even though they are not, as they largely play on the psyche and tech-savviness of the consumer, making it far more sinister than usual deceptive techniques. Dark Patterns play on the psychological weaknesses and shortcomings of consumers.

---

[2] Central Consumer Protection Authority, Guidelines for Prevention of Misleading Advertisements and Endorsements for Misleading Advertisements (June 2022).
[3] Harry Brignull, 'Bringing Dark Patterns to Light' (*Medium*, 7 June 2021) <https://harrybr.medium.com/bringing-dark-patterns-to-light-d86f24224ebf> accessed 1 January 2024.
[4] consumer Protection Act, 2019, s 2(47).

Referring to Tversky & Kahneman's Dual Process Theory, it is suggested that humans have two modes of thinking: 'System 1' and 'System 2.'[5] The attributes of these two are expressed below graphically:

SYSTEM 1 THINKING

Prompt
Unconscious
Automatic
Less Laborious
Less Rational

SYSTEM 2 THINKING

Conscious
Rational
Laborious

According to research, consumers are more likely to make rash decisions that are better for the interests of the providers than their own since dark patterns appeal to 'System 1' of the human brain.[6] Rather than being persuasive, dark patterns tend to be manipulative, targeting largely children and old people with limited or diminished psychological ability.

Many dark patterns like subscription traps, confirm shaming or trick questions may appear standard at the first instance, when in fact they are practices devised to take advantage of customers. E.g. subscription trap, makes it cumbersome and difficult for consumers to cancel their subscription to any app or website by hiding the cancel button or making the consumer go through many tabs and tasks to cancel subscriptions while the process to subscribe is usually much easier and convenient.

At first glance such patterns may not seem irregular or of much concern since the website does offer its consumers the choice to opt-out or unsubscribe, making it difficult but not impossible to do so. However, the trap works at the psychological level by making the consumers tired of trying to find the 'cancel button' or complete the formalities of unsubscribing. Hence, discouraging them from opting out and manipulating them into recurrently paying for services which they do not need. A pertinent example of this would be the Federal Trade Commission (USA) filing a lawsuit against Amazon Inc. for enrolling their customers in the 'Prime program' without getting their express, informed consent and making it difficult for them to rescind or unsubscribe from the said service.[7] Usual provisions on unfair trade practices fall short of addressing deceptions like that.

Similarly, websites 'confirm shaming' their users into purchasing by inducing 'ridicule' or 'guilt' or 'fear' in the mind of the consumer might not, on the surface, appear to be an unfair trade practice

[5] A. Tversky & D. Kahneman, 'Judgment under Uncertainty: Heuristics and Biases' (1974) 185 Science 1124, 1131.
[6] C. Bosch et al., 'Tales from the Dark Side: Privacy Dark Strategies and Privacy Dark Patterns' (2016) Proceedings on Privacy Enhancing Technologies, 237, 254.
[7] 'FTC sues Amazon for tricking customers into signing up for Prime' (*The Verge*, 21 June 2023) <https://www.theverge.com/2023/6/21/23768372/ftc-amazon-lawsuit-prime-dark-patterns-subscriptions> accessed 25 December 2023.

since it does not 'rob' the consumer of the choice to opt-out. However, when we take into account the psychological aspect of the confirmation bias it imposes, the deception becomes clear.

An appropriate example of this would be companies providing antivirus and data security applications like McAfee who 'persuade' their users into buying subscriptions of their product by showing prompts like 'Renew' or 'Accept Risk', manipulating the consumer into believing that they are prone to imminent data security threats by not buying their product. The picture below is taken from the personal experience of the author, who has received this pop-up message multiple times on their device.

Figure 1 (McAfee Anti-Virus Renewal Pop-up)

Thus, to answer the question, separate laws are indeed required for Dark Patterns since most laws relating to unfair trade practices are inept at dealing with deceptions through user interface or user experience that play with the psychological vulnerabilities of consumers, manipulating them into making choices that they otherwise wouldn't.

III. Indian Guidelines On Dark Patterns:

Before delving into various dark pattern laws around the world, it is necessary to gauge what the Guidelines issued by the CCPA say.

A. APPLICABILITY:

- All platforms offering goods and services in India[8];
- Advertisers[9];
- Sellers[10].

From the first clause, it is clear that these guidelines apply to all companies providing services in India, whether domestic or foreign, amplifying the scope of these guidelines. The guidelines

[8] Central Consumer Protection Authority, *Guidelines on Prevention and Regulation of Dark Patterns* (November 2023), s 3.
[9] ibid.
[10] ibid.

prohibit any person, including any platform from engaging in 'Dark Pattern' practices. In the event any person (including a platform) engages in the Dark Patterns specified in Annexure I to the guidelines, such person (or platform) will be considered as engaging in a dark pattern practice.[11] And be liable for the same.

B. SPECIFIED DARK PATTERNS:

Annexure I of the Guidelines specify 13 major dark patterns while CCPA has the discretion to include more from time to time.

The dark patterns identified as of now are:

False urgency

It is characterized by fabricating or suggesting a false sense of urgency or scarcity in order to deceive a customer into buying something or acting right away when they otherwise wouldn't have. False urgency usually involves displaying false popularity of a product or service or showing that there are fewer available units of specific goods or services than there are.[12]
Now some common examples of false urgency are e-commerce websites conveying to consumers that they only have a few pieces of an item left in their inventory in which the consumer seems interested, in order to induce them to make the purchase. This has also been the case with travel websites manipulating customers into making a purchase by displaying false urgency. The picture below is a screenshot of a notification received by the author on their device.

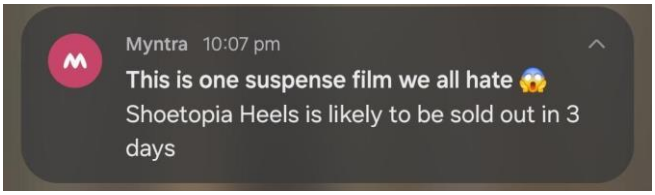

Figure 2 (Myntra Notification)

Here, we can see that the e-commerce website, Myntra, has created a sense of urgency and scarcity to induce the consumer to hurriedly make a purchase.

Basket sneaking

It involves including extra items such as products, services or payments to charities/donations at the time of payment or checkout from a platform without the consent of the consumer which results in an increase in the amount payable by them. This guideline provides exceptions for certain items like free samples or complimentary services or the addition of necessary fees such as delivery charges, wrapping charges and taxes, at the time of checkout.[13]
This has been a massive issue with travel booking websites pre-selecting travel insurance coverage as a default option while buying travel tickets which compelled the Insurance Regulatory and

[11] ibid s 5.
[12] Central Consumer Protection Authority, *Guidelines on Prevention and Regulation of Dark Patterns* (November 2023), Annexure 1, cl 1.

[13] Ibid cl 2.

Development Authority of India (IRDAI) to instruct insurers that travel insurance policy option should not by default be pre-selected at the time of checkout and that no insurance can be bought 90 days before travel.[14] This was a welcome step towards transparency since oftentimes, the consumers were buying travel insurance without even being aware of it and hence not being able to use it in times of need, defeating the purpose of such insurance.

Confirm shaming

It refers to the use of images, sounds, phrases or any other technique to instil in the user a sense of 'guilt', 'shame', 'fear', or 'ridicule' to persuade them to act in a way that will lead to them buying goods or services from a platform or renewing their subscription to a service.[15]

An example of such 'confirm shaming' done by anti-virus software companies (Figure 1) has been given above in this paper.

Forced action

This entails forcing consumers into purchasing any additional good(s) or enrolling for an unrelated service to buy or subscribe or avail of the product or service they originally intended to purchase.[16]

Some examples of this would be forcing consumers to share their sensitive personal information such as Aadhar card details.[17] or credit card or biometric information[18] Even when such data is not necessary for the transaction or forcing them to download unrelated apps while availing a service.

Subscription trap

It includes barriers to cancellation of a paid subscription. Here, the process to cancel is made impossible or lengthy by hiding the option to cancel; or compelling a consumer to provide payment details and/or consent for auto debits to avail free subscriptions, along with making the instructions to cancel confusing, cumbersome or ambiguous.[19]

Amazon Prime enrolling its customers in its 'Prime Program' without their informed consent and making the process to unsubscribe difficult would be a relevant example.[20] It has also been discussed previously in the paper.

Interface Interference

[14] Insurance Regulatory and Development Authority of India, *Circular on Travel Insurance Products and operational matters* (September 27, 2019).
[15] *Central Consumer Protection Authority* (n 12) cl 3.
[16] *Central Consumer Protection Authority* (n 12) cl 4.
[17] Nidhi Singhal, 'Aadhar not mandatory yet organisations pose it as a mandatory document' *Business Today* (India, 29 May 2022) < https://www.businesstoday.in/latest/trends/story/aadhaar-not-mandatory-yet-organisations-pose-it-as-a-mandatory-document-335550-2022-05-29> accessed 6 October 2024.
[18] Sneha Kulkarni, 'This new Aadhaar-related banking fraud is on the rise; why you need to lock your Aadhaar biometrics now' *Economic Times* (India, 20 October 2023) <https://economictimes.indiatimes.com/wealth/save/this-new-aadhaar-related-banking-fraud-is-on-the-rise-why-you-need-to-lock-your-aadhaar-biometrics-now/articleshow/104575645.cms?from=mdr> accessed 6 October 2024.
[19] *Central Consumer Protection Authority* (n 12) cl 5.
[20] FTC sues Amazon for tricking customers into signing up for Prime (n 7).

This entails a design element on a website intended to a) highlight certain specific information and/or b) obscure any other relevant information, tricking consumers into taking an action desired by the creator of such design.[21]

A prime example of interface interference is 'cookies consent notices' on various websites. Cookie consent notices use methods like interface interference which includes 'aesthetic manipulation'. Aesthetic manipulation involves using 'high-contrast' colours on texts and larger fonts that the designers would want the users of that website to see and choose (like the option to 'Accept Cookies') but minimizing or hiding crucial information[22] or displaying other options with misleading colours like grey to give the impression that they cannot be selected or are invalid are common methods of dark patterns employed by websites to extract private information from users.

The visual given below was discovered in an article on 'Cookie Consent notices' highlighting the usage of dark patterns in them.[23]

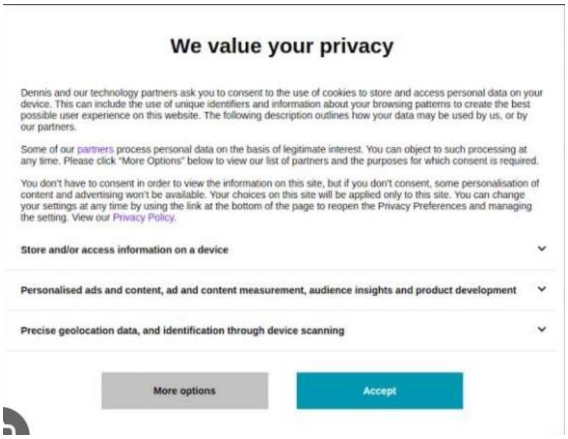

Figure 3 (autoexpress.co.uk)

Bait and Switch

It describes the tactic of advertising a particular outcome based on the user's action but misleadingly serving an alternate outcome.[24]

An example of this would be when a user selects a product at a particular price but at the time of checkout that product is no longer available and a substitute product is offered which is costlier than the product chosen, again a common sight at travel booking websites.[25]

Drip Pricing

[21] *Central Consumer Protection Authority* (n 12) cl 6.
[22] Danyang Li, 'The FTC and the CPRA's Regulation of Dark Patterns in Cookie Consent Notices' (2023) 1 U Chi L Rev <https://businesslawreview.uchicago.edu/sites/default/files/2023-03/Li_v1n19_561-590.pdf.> accessed 26 December 2023.
[23] Colin M. Gray and others, 'Dark Patterns and the Legal Requirements of Consent Banners: An Interaction Criticism Perspective' (2021) CHI Conferences on Human Factors in Computing System (CHI'21) <`https://doi.org/10.1145/3411764.3445779> accessed 26 December 2023.
[24] *Central Consumer Protection Authority* (n 12) cl 7.
[25] Chris Baraniuk, 'How 'dark patterns' influence travel bookings' *BBC* (UK, 12 Dec. 2019) <https://www.bbc.com/worklife/article/20191211-the-fantasy-numbers-that-make-you-buy-things-online> accessed 6 October 2024.

Drip pricing[26] Usually affects the prices payable by consumers. It involves:

- keeping elements of prices secretive and not revealing them upfront to the consumers or revealing them stealthily within the user experience; or
- informing the consumer of the actual price post-confirmation of the purchase, that is, charging more than what was disclosed at the time of payment; or
- advertising a product or a service as free without disclosing that further usage necessitates in-app payments; or
- preventing a consumer from utilizing a service for which he has already paid, without making additional purchases.
- These guidelines do not put any liability on a marketplace e-commerce entity for price fluctuations caused by price changes effected by third-party sellers or due to any other external factor outside of their control.
- Drip pricing is usually seen in gaming apps which advertise themselves as free but their continued usage requires app purchases. The maker of the game 'Fortnite', Epic Games had to shell out $520 million in settlement to FTC for duping players, especially children into buying in-game cosmetics.[27]
- Disguised Advertisement
- It refers to a practice of masking or disguising advertisements as other types of content like user-generated content false advertisements new articles etc.[28]
- The guideline states that the term 'disguised advertisement' also includes 'misleading advertisement' as provided under Section 2(1)(28) of the CP Act.[29] and the "Guidelines for Prevention of Misleading Advertisements and Endorsements for Misleading Advertisements, 2022[30]" shall also apply to it. Here, it is the responsibility of the seller or advertiser to make such disclosure on the platform.
- A common example of this is influencers making content on a particular product or service which is an advertisement but not explicitly disclosing that such content is an advertisement to their followers and target consumers.[31] To curb this issue, the Advertising Standards Council of India (ASCI) also had to roll out guidelines on Influencer Advertising in Digital Media.[32]

Nagging

[26] *Central Consumer Protection Authority* (n 12) cl 8.
[27] 'FTC Finalizes Order Requiring Fortnite maker Epic Games to Pay $245 Million for Tricking users into Making Unwanted Charges' (*Federal Trade Commission*, 14 March 2023) <https://www.ftc.gov/news-events/news/press-releases/2023/03/ftc-finalizes-order-requiring-fortnite-maker-epic-games-pay-245-million-tricking-users-making> accessed 26 December 2023.
[28] *Central Consumer Protection Authority* (n 12) cl 9.
[29] Consumer Protection Act, 2019, s 2(1)(28).
[30] *Central Consumer Protection Authority* (n 2).
[31] Anupriya Chatterjee, 'Attention influencers. You may soon be fined lakhs for false ads, or not disclosing paid content' *ThePrint* (India, 17 Sept. 2022) < https://theprint.in/india/governance/attention-influencers-you-may-soon-be-fined-lakhs-for-false-ads-or-not-disclosing-paid-content/1130496/> accessed 6 October 2024.
[32] The Advertising Standards Council of India, *Guidelines for Influencer Advertising in Digital Media,* (1 June 2021).

Nagging as a dark pattern involves flooding users with requests, options, pop-ups or any other interruption unrelated to the action of purchasing goods or services intended by the consumer. Such requests most often disrupt the intended transactions. Nagging behaviours intend to obstruct the usage or visibility of the interface or distract and redirect the attention of the user.[33]

Nagging again is a pattern which a lot of consumers have experienced on apps which give prompts for turning on notifications or collecting any sort of personal data. Instead of giving the consumer a choice between 'Yes' or 'No', the consumer is compelled to choose between 'Yes' and something like 'Maybe Later' or 'Not now', making the consumer prone to such pop-ups in their in-app experience. The visual given below is yet another example of Nagging, it was presented as an item in California Privacy Protection Agency's Pre-Rule Making Informational sessions.[34]

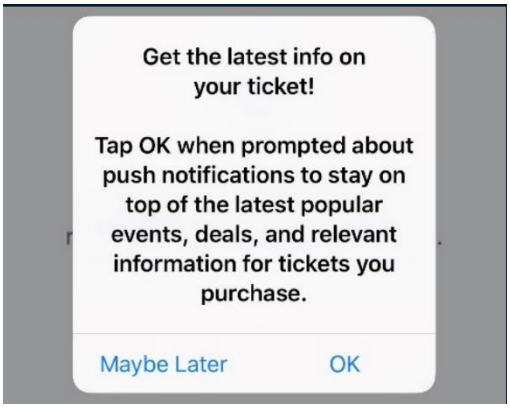

Figure 4 (ccpa.ca.gov)

Trick Question

The term trick question refers to the purposeful use of ambiguous or misleading language, such as 'double negatives' or 'unclear terminology' or other similar techniques to deceive or mislead a consumer from doing desired actions or persuade them to adopt a particular response or action.[35] Trick questions are designed to play on the attention deficit of the consumers while clicking through various boxes out of habit expecting the same prompts.

By using 'asymmetric' or 'double negative' language, they trick consumers into performing tasks such as 'accepting spam emails' or calls which the consumer wouldn't have intended to.

Saas Billing

[33] *Central Consumer Protection Authority* (n 12) cl 10.
[34] Dr. Jennifer King, 'Dark Patterns & Manipulative Design' (*California Privacy Protection Agency,* 29 March 2022) <https://cppa.ca.gov/meetings/materials/20220329_30_day_1_item_2c_king.pdf> accessed 31 December 2023.
[35] *Central Consumer Protection Authority* (n 12) cl 11.

It involves collecting payments from consumers recurrently and as surreptitiously as possible.[36] Saas billing is often combined with Subscription trap where the consumer is tricked into continuing with the subscription of a good or service, like subscription to 'OTT Platforms' where options of auto-renewal or auto-debit are 'pre-selected' or difficult to remove and consumers are not provided any choice in changing such settings.

Rogue Malwares

As per the guidelines, 'Rogue Malwares' means using a 'ransomware' or 'scareware' to deceive consumers into thinking that there is a virus or malware on their electronic device and consequently convincing them to purchase a fake malware removing tool or software which then actually installs malware on the device of the consumer.[37]

This is a common sight on pirated websites which often show pop-ups like 'Warning!' or 'Virus Detected' to scare consumers into taking actions such as purchasing their fake software and subsequently losing their data. The visual given below is a prime example of 'Rogue Malware' in dark patterns.[38]

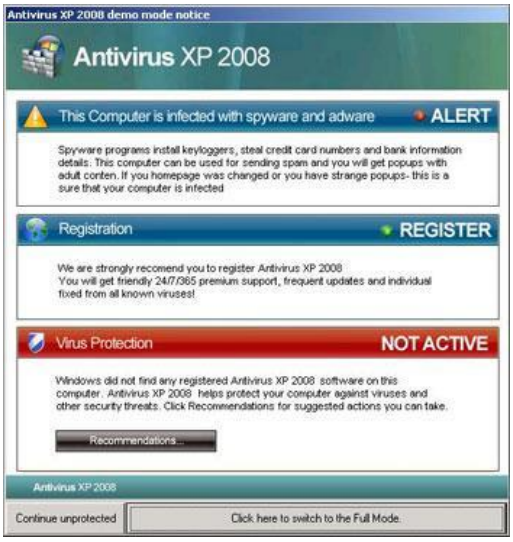

Figure 6 (bumc.bu.edu)

Hence, these are the dark patterns identified by the Indian regulations as of now. These guidelines underscore the commitment on the part of the government to protect consumer autonomy in the digital eco-space along with safeguarding their privacy, by placing significant emphasis on creation of reasonable user interface, especially in light of the linkage between dark patterns and user content in the privacy regime.[39]

---

[36] *Central Consumer Protection Authority* (n 12) cl 12.
[37] *Central Consumer Protection Authority* (n 12) cl 13.
[38] 'Rogue Security Software' (*Boston University Medical Campus Information Technology)* <https://www.bumc.bu.edu/it/infosec/prevention/rogue/> accessed 5 January 2024.
[39] Bhuvnesh Kumar and Sharad Panwar, 'Navigating Deception: Dissecting the Implications of India's Guidelines on Dark Patterns' (*The Wire, 5* December 2023) < https://thewire.in/rights/india-guidelines-dark-patterns-implications> accessed 30 December 2023.

Liabilities And Punishment For Engaging In Dark Patterns:

The CP Act imposes severe fines and imprisonment[40] on the usage of any of the Dark Patterns mentioned in 'Annexure 1' of the Guidelines. Imprisonment for up to six months; a fine of up to Rs. 20 lakhs, or both for non-compliance with the Act's directions. Imprisonment for up to two years and a fine of up to Rs. 10 lakhs can also be imposed additionally for creating/causing false or misleading advertisementswhich are prejudicial to the interests of the consumers. The imprisonment and fine can increase for subsequent offences.

Can Commercial Entities Sue Under The Dark Patterns Regulations?

After reviewing the guidelines, a valid question that arises is whether commercial entities can sue for infringement of autonomy and choice under these regulations. For this, reliance has to be placed upon the definition of 'consumers' in the CP Act, which is the parent Act. The Act defines a 'consumer' as "a person who buys any goods or services for a consideration, which has been paid or promised or partly paid and partly promised, or under any system of deferred payment also includes the user with approval of such goods or beneficiary of services"[41]. The definition excludes any person who avails services for any commercial purposes. It needs to be noted that the definition of 'consumer' given by the Consumer Protection Act, 1986[42] is similar to the 2019 Act on these accounts.

The Supreme Court has held that the definition of 'consumer' under the CP Act, 1986 includes a commercial entity provided that the goods purchased, or services availed are not linked to any profit generating activities or commercial purposes.[43] Considering this, it won't be incorrect to say that commercial entities too can seek remedy against dark patterns under these regulations, given that the activity which has been vitiated by dark patterns is an activity not directly intended to generate profit for the concern.

IV. Dark Patterns Regulations: A Global Perspective

India is not the only country with Dark Patterns laws in place. Any analysis of Dark Pattern regulations would be incomplete without a global perspective on the same. Hence, the author attempts to analyze, summarise and compare laws on dark patterns in different international jurisdictions such as the European Union (EU), United States of America (USA), Australia, South Korea and Argentina with that of India.

European Union (EU)

[40] *Consumer Protection Act* (n1) s 21.
[41] *Consumer Protection Act* (n 1) s 2(7).
[42] Consumer Protection Act, 1986, s 2(1)(d).
[43] *National Insurance Co. Ltd. v Harsolia Motors & Ors.* 2023 SCC OnLine 409.

The European Union has regulations on Dark Patterns. Dark patterns are mentioned or referred to in the General Data Protection Regulations[44] ("GDPR"), the Digital Services Act[45] ("DSA") and the Unfair Commercial Practices Directive ("UCPD")[46]. Recital 67 of the DSA defines dark patterns as "practices that materially distort or impair, either on purpose or in effect, the ability of recipients of the service to make autonomous and informed choices, or decisions. Those practices can be used to persuade the recipients of the service to engage in unwanted behaviours or into undesired decisions which have negative consequences for them." [47]

DSA prohibits providers of online platforms from impairing or distorting the autonomy, choice and decision-making of 'recipient of services' by deceiving or nudging them through structure, design or functionality of any UI/UX or part thereof. While this provision doesn't specify or name any particular dark pattern but it does lay down certain actions or designs or patterns that can be categorized as dark patterns. They are:

- Design choices that are exploitative and compel the recipient to perform actions that might not be in their best interests but which serve the providers of online platforms;
- Presenting certain choices in a more prominent manner through audio or visual or any other aid when asking the user to make a certain choice or action. Here, the choices are presented in a non-neutral way to exploit cognitive biases of the consumer;
- Nagging, that is, flooding recipients of the service with requests of making a choice where such choice has already been made;
- Providing barriers to cancellation of a particular service or subscription by making the process of cancellation much lengthy and cumbersome than the process to sign up or making certain actions more difficult and time-consuming than others or making it unnecessarily difficult to opt-out of purchases or sign out from any online platform allowing remote contact with traders;
- Using default settings on online interface which can be very difficult to change and have the capacity to irrationally bias the decision-making of a recipient of service or deceiving such recipients by compelling them to make any decision in a transaction which might not be in their best interests.

This definition of dark patterns has wide implications because anything on an online interface of an online platform that can "materially distort or impair the ability to make autonomous and informed choices" of the consumers or recipients can be called a Dark Pattern. The definition

[44] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L 119/1.
[45] Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on the Single Market for Digital Services and amending Directive 2000/31/EC (Digital Services Act) [2022] OJ L 277/1.
[46] Commission Notice 2021/9320 of 29 December 2021 on the Guidance on the interpretation and application of Directive 2005/29/EC of the European Parliament and of the Council concerning unfair business-to-consumer commercial practices in the internal market [2005] OJ L 149/22.
[47] *Digital Services Act* (n 45) recital 67.

focusses heavily on consumer autonomy and ability to make choices which again alludes to the psychological effect of dark patterns and their ability to manipulate the psyche and decision-making process of the consumer.

While the Act does not give an exhaustive list of dark patterns like the Indian guidelines but the definition certainly describes some dark patterns like Interface Interference, Trick Question, Nagging, Subscription Trap with the list not being exhaustive. User interfaces which deceive or mislead recipients or encroach upon their ability to make free and informed decisions shall be prohibited under Article 25 of the DSA[48] and in light of such restrictions, providers will have to re-evaluate their platforms.

GDPR does not directly mention dark patterns but it needs to be credited for laying down the essential regulatory framework. Article 25 sub-clauses 1 and 2 talk about the maintenance of privacy by data controllers in their interfaces by default as well as by design.[49] The provision can be construed to protect the consumers from unfriendly default settings, imperceptible decline options and strategies to guilt the consumer to compromise personal data. However, the same cannot be viewed as a holistic mechanism to regulate dark patterns.[50] While it might not have been a complete mechanism, it provided a layout for personal data protection of the consumers which often is at the receiving end due to dark pattern practices by operators who manipulate consumers into giving up their details by exploiting cognitive biases (like cookie consent notices).
UCPD lays down the general infrastructure which regulates business-to-consumer (B2C) relationships along with restricting practices which are unfair. UCPD applies to both online and offline sellers, making it technologically neutral. Dark Patterns have been extensively mentioned in the Commission's 2021 Guidelines,[51] making such practices liable to be challenged under the UCPD as well. Dark Patterns like 'Bait and Switch', 'Fake limited Stock Claims', 'Fake timers' and 'Nagging' have been blacklisted under Annex 1. The UCPD's standard reasoning would be applicable for any other pattern: "If significant information is withheld or presented in a way that influences the consumer to make a decision they otherwise would not have made, that behaviour would be considered a misleading Dark Pattern practice." Alternatively, if the pattern impairs consumer autonomy through use of force, coercion or undue influence impelling them to make undesirable choices, it may be characterized as aggressive.[52]

The EU framework on dark patterns is a triad of three acts- UCPD, GDPR and DSA. It is possible to say that Dark Patterns have been construed as a subset of Data Protection Laws and Consumer

[48] *Digital Services Act* (n 45) art. 25.
[49] *General Data Protection Regulation* (n 44) art. 25 cl 1 & 2.
[50]Jamie Lugiri and Lior Strahilevitz, 'Shining a Light on Dark Patterns' (2021) 13 J Leg Anal <https://ssrn.com/abstract=3431205> accessed 30 December 2023.
[51] Commission Notice (EU) 2021/C 526/01 of 29 December 2021 laying down Guidance on the interpretation and application of Directive 2005/29/EC of the European Parliament and of the Council concerning unfair business-to-consumer commercial practices in the internal market [2021] OJ C 526/1.
[52] Tom Akhurst and others, 'How Should the European Union Regulate Dark Patterns?' (2023) Sciences Po Chair Digital Governanance and Sovereignty Student's Policy Brief, <https://www.sciencespo.fr/public/chaire-numerique/en/2023/09/12/students-policy-brief-how-should-the-european-union-regulate-dark-patterns/> accessed 29 December 2023.

Protection Laws. This is one aspect in which the Indian jurisdiction differs, since the Indian laws have fallen short of recognizing the 'right to privacy'[53] as a consumer right.

The guidelines still do not address the various risks, in particular, the threat posed by the unauthorized collection of excessive and unnecessary personal data without informed consent of users. Dark patterns have been closely linked to privacy and consumer autonomy in EU jurisprudence through their inclusion in data protection acts while dark pattern regulations in India have strictly remained 'unfair trade practices' without tapping deep into the data protection aspect of it. Even the Digital Personal Data Protection Act[54] of India fails to adequately govern and restrict User Interface tasked with collecting personal data of consumers.
Secondly, the DSA doesn't place emphasis on the 'intention to mislead' while determining liability for websites using dark patterns in their interface, any feature adversely affecting consumer choice can be considered one, the intention of the provider behind it is inconsequential (Recital 67). Liability is also attracted if the platform or business knows that it has the effect of manipulating or 'subverting' a user's choice and does not remedy the same, but in India, one necessary ingredient to establish that a user interface uses dark patterns is to prove that it was 'designed to mislead'. While the requisition to prove intention behind the design of any UI/UX interface can be a useful tool to ensure that a detailed analysis is carried out, it can also become difficult to establish an 'intention to mislead' in each and every case. Thus, it remains to be seen how the Central Consumer Protection Authority interprets and enforces this.[55]

On a comparative note, the two major places where the regulations on dark patterns differ in both the jurisdictions is on the emphasis of personal data protection of consumers and the essentiality of presence of intention to mislead.

The United States Of America

There has been a crackdown on dark patterns by various authorities in the USA, especially the Federal Trade Commission (FTC). The FTC's April 2021 workshop 'bringing dark patterns to light' investigated manipulative user interface designs on websites and Apps. It was the first federal authority to do so in the states. It further put out it's 'Bringing Dark Patterns to Light'[56] report in September 2022 elucidating on how intricate design practices are being employed by organisations to manipulate or mislead consumers into buying products and services or giving up their personal information. The report highlighted various Dark Patterns in UI/UX like[57]:

1. **URGENCY** which consists of 'Baseless Countdown Timer', 'False Limited Time Message' and 'False Discount Claims'.

[53] *Justice K.S. Puttaswamy & Anr. v Union of India & Ors.* AIR 2017 SC 4161.
[54] The Digital Personal Data Protection Act, 2023.
[55] Paritosh Chauhan and Rohan Verma, 'Regulation of Dark Patterns' (*Lakshmikumaram & Sridharan Attorneys,* 19 December 2023) < https://www.lakshmisri.com/insights/articles/regulation-of-dark-patterns/#> accessed 30 December 2023.
[56] FTC Bureau of Consumer Protection, 'Bringing Dark Patterns to Light' (FTC Staff Report 2022).
[57] ibid Appendix A.

2. **OBSTRUCTION** which includes 'Price Comparison Prevention', 'Roadblocks to Cancellation' and 'Immortal Accounts'.
3. **SNEAKING OR INFORMATION HIDING** which includes 'Sneak into Basket', 'Hidden Information', 'Hidden Costs', 'Drip Pricing', 'Hidden Subscription' or 'Forced Continuity' and 'Intermediate Currency'.
4. **INTERFACE INTERFERENCE** which consists of 'Misdirection', 'False Hierarchy', 'Disguised Ads' and 'Bait and Switch'.
5. **COERCED ACTION** entailing 'Unauthorized transactions', 'Auto-play', 'Nagging', 'Forced Registration or Enrollment', 'Pay to play' and 'Friend Spam/Social Pyramid Schemes'.
6.
7. **ASYMMETRIC CHOICE** including 'Trick Questions', 'Confirm Shaming', 'Preselection, Subverting Privacy, Preferences'.

While the USA does not yet have a federal law or regulation on Dark Patterns yet, a number of states have adopted such regulations. The first one to do so is California through the California Consumer Privacy Act[58] ("CCPA") and California Privacy Rights Act[59] ("CPRA"), the state of Colorado through Colorado Privacy Act[60] ("CPA") and Connecticut through Act Concerning Personal Data Privacy and Online Monitoring, also known as the Connecticut Data Privacy Act.[61] All these acts expressly restrict the use of dark patterns.

CCPA's recently updated regulations state that "a business shall not use a method that is designed with the purpose or has the substantial effect of subverting or impairing a consumer's choice to opt-out".[62] This has been made in consonance with the new privacy rights introduced for California consumers such as the 'right to opt-out' of the sale or sharing of their personal information or the 'right to delete' personal data collected from them or the 'right to know' about the personal data which a business collects about them and how it is used and shared.[63] It is pertinent to note that as per the regulation any platform or seller hosting a website with UI/UX which utilizes Dark patterns shall be liable under the act, the 'intention' to mislead or subvert the choice of the consumer is inconsequential.

The CPRA defines dark patterns as "user interface designed or manipulated with the substantial effect of subverting or impairing user autonomy, decision-making or choice, as further defined by regulation". If a platform contains any user interface that subverts the autonomy or decision-making of a consumer and the platform provider is aware of it, then the provider shall be liable for engaging in dark pattern usage even though such usage was unintentional, i.e., the platform was not

[58] California Consumer Privacy Act, 2018 (USA).
[59] California Privacy Rights Act, 2020 (USA).
[60] Colorado Privacy Act, 2021 (USA).
[61] Connecticut Data Privacy Act, 2022 (USA).
[62] Dr. Jennifer King (n 34).
[63]'California Consumer Privacy Act' (*State of California-Office of Attorney General*, 10 May 2023) <https://oag.ca.gov/privacy/ccpa#:~:text=Are%20there%20any%20CCPA%20regulations,the%20California%20Privacy%20Protection%20Agency.> accessed 31 December 2023.

designed with the 'intention to mislead'. Similarly, a business' willful ignorance of the impact of its user interface may also support the establishment of a dark pattern.[64]

Several requirements have been laid down along the lines of which businesses are supposed to implement methods for submitting CCPA requests and obtaining consumer consent for various purposes like collecting their personal data such as making options 'easy to understand', ensuring 'symmetry in choice' (for eg. providing options like 'Yes' and 'Ask me Later' are asymmetrical since the consumer is not given any option to decline the opt-in), 'avoiding confusing language' etc.[65]

Alongside CPRA, the Colorado Privacy Act makes explicit mention of dark patterns calling it "a user interface designed or manipulated with substantial effect of subverting or impairing user autonomy, decision making or choice." Connecticut's Data Privacy Act also mentions dark patterns. It explicitly excludes dark patterns in its definition of 'consent'. This flows from the school of thought that consent should be freely given, informed, unambiguous and free from any external pressure like coercion, fraud or undue influence. Dark Patterns shall include but not be limited to any practice that the FTC deems as one.[66]

While comparing the regulations in American and Indian jurisdictions, a stark difference that can be noted is that the American Regulations are more concerned with the Protection of Personal Data and ensuring consumer's 'right to opt-out' of sharing such data and refusing platforms the right to sell such data, while the regulations in the Indian jurisdiction aim at preventing unfair trade practices and practices that might be prejudicial to consumers as such. The Indian counterpart lacks specific focus on the effect of dark patterns in collecting personal data and measures to stop it. This angle of legislation is yet to be traversed by the Indian lawmakers.

Secondly, the American legislation too, like EU, states that a platform shall be liable for UI/UX utilizing dark patterns irrespective of the fact whether it was the platform or designer's intention to mislead the consumer. The American legislation takes a more consumer-oriented approach by making businesses liable even if they ignore to rectify such dark patterns or lack intention to use dark patterns while the Indian legislation takes a neutral ground by making the 'intention to mislead' or 'designed to mislead' an essential for proving liability.

Australia

Australia does not have any specific law on Dark Patterns yet but it is governed by the Australian Consumer Law ("ACL"). Schedule 2 of the Competition and Consumer Act[67], (formerly known as the Trade Practices Act, 1974) contains the ACL. While dark patterns are not automatically illegal in Australia but to combat their usage in the marketplace, the Australian Competition and Consumer Commission ("ACCC") which is in charge of enforcing the ACL has implemented a number of

[64] California Privacy Rights Act, s 7004 (c).
[65] ibid s 7004 (a).
[66] Connecticut Data Privacy Act, s 1(11).
[67] Competition and Consumer Act, 2012 sch. 2 (Aus).

measures. Similar to how the Federal Court ordered ticket reseller 'Viagogo AG' to pay $7 million in penalty for violating ACL by reselling tickets for live music or sporting events under false or misleading representations, in an action brought by ACCC. The company was misleading consumers by creating a 'false sense of urgency' by implying that tickets were scarce and by marketing tickets at a lower cost by not including the necessary, unavoidable fees.[68]

ACL contains protections against 'misleading or deceptive conduct'[69], 'unconscionable conduct'[70] and 'unfair terms'[71] which can be used against dark patterns. Additionally, it offers defense against a range of practices that can be considered dark patterns such as demanding payment for an unsolicited good or service[72] (e.g. 'basket sneaking'), not clearly displaying the total cost of a product or a service[73] (e.g. 'drip pricing'), or bait advertising[74] ('bait and switch').

The Privacy Act, 1988[75] establishes stringent guidelines for the collection, use and storage of personal data.[76] Among these guidelines is the requisition that people must be made aware of their rights, and the nature of the data collected and the purpose for which data will be used. Further, using ambiguous language ('trick questions') in terms and conditions or privacy policies which deceive consumers into disclosing their personal information without being fully informed of their rights can also count as a violation of ACL.[77] Dark Patterns have been flagged and punished in Australia but the laws are still not as comprehensive and specific as in the Indian jurisdiction. Some dark patterns like false urgency or basket sneaking or bait and switch are already included in the ACL but the presence of a specific piece of legislation adds an extra layer of enforceability and awareness on such practices especially for consumers, who might mistake it as a norm on websites.

South Korea

The Korea Fair Trade Commission ("KFTC") on April 21, 2023 released the 'Policy Direction for Protecting Consumers from Online Dark Patterns'.[78] South Korea has been one of the few jurisdictions to come out with a comprehensive plan to tackle dark patterns. The Consumer Protection in Electronic Commerce, 2012 ("E-Commerce Act") ensures consumer protection on e-commerce platforms. This Act's purpose is to safeguard consumer rights and interests by establishing guidelines for fair trade of goods and services through mail order, e-commerce transactions and other channels.[79] The Policy guidelines are a welcome move to remove any doubts on what counts as dark patterns, since the broad language of Article 21 Paragraph (1), Item 1 of the

---

[68] 'Viagogo to pay $7 million for misleading consumers' (*ACCC*, 2 October 2020) <https://www.accc.gov.au/media-release/viagogo-to-pay-7-million-for-misleading-consumers> accessed 1 January 2024.
[69] Australian Consumer Law, s 18.
[70] ibid s 20.
[71] ibid s 23.
[72] ibid s 40.
[73] ibid s 48.
[74] ibid s 35.
[75] The Privacy Act, 1988 (Aus).
[76] 'Privacy' (*Australian Government-Attorney General's Department)* < https://www.ag.gov.au/rights-and-protections/privacy#:~:text=The%20Privacy%20Act%201988%20(Privacy,and%20in%20the%20private%20sector.> accessed 6 October 2024.
[77] 'Dark Patterns: User interfaces that make consumers buy and buy more. What are the laws and are dark patterns legal?' (*Sharon Giovani Consulting*, 18 January 2023) <https://sharongivoni.com.au/dark-patterns-user-interfaces-that-make-consumers-buy-and-buy-more-what-are-the-laws-and-are-dark-patterns-illegal/> accessed 1 January 2024.
[78] Korean Fair Trade Commission, *Policy Direction for Protecting Consumers from Online Dark Patterns*, (21 April, 2023) (SK).
[79] Act on the Consumer Protection in Electronic Commerce, 2012 art. 1.

E-Commerce Act[80] which prohibits companies from "luring customers, concluding a deal with consumers, or interfering with customer's cancellation, etc. or orders or termination of contracts by providing false or exaggerated information or by deceptive means" still has more to cover when it comes to dark patterns.[81] Currently, the National Policy Committee of South Korea has introduced five amendment bills pertaining to dark patterns, four of which aim to amend the E-Commerce Act and one of which seeks to amend the Personal Information Privacy Act ("PIPA").

The following amendments are to be introduced in the E-Commerce Act[82]:

- Mandating e-commerce businesses to disclose to customers any modifications to the fee structure (such as turning free trials into paid subscriptions) or charging increased fees, as well as the total amount that a customer must pay. The bill also prohibits 'drip pricing', 'bait and switch', 'preselection', 'roadblocks to cancellation' and 'nagging'.
- Prohibiting e-commerce businesses from processing recurring payments without the consumer's consent, tricking consumers into agreeing to such recurrent payments, or meddling with account cancellation.
- Mandating e-commerce businesses to create UI that can prevent or lessen the damage caused by user errors.
- Prohibiting e-commerce businesses from manipulating or altering User Interface designs in order to impede consumers from making informed decisions.
- Proposed amendments in PIPA[83]:
- Prohibiting personal information controllers from gathering personal data by coercing consumers into making unintended choices or decisions that violate their rights.[84]

The following amendments that are sought to be introduced are common trends noticed in all jurisdictions which have started regulating dark patterns. The most common dark pattern that has been referenced is 'subscription trap' which also includes SaaS billing. Other commonalities include making the UI design easier and avoiding trick questions while collecting personal data of consumers. The KFTC also released the 'Guidelines on the Voluntary Management of Online Dark Patterns'[85] on July 31, 2023 as a way to supplement the policy directions. The guidelines have categorized dark patterns into 4 main categories and 19 distinct types. The Indian guidelines had defined 13 major dark patterns, but the Korean guidelines move a step further and identify 19 distinct types with 'False Discount Claims', 'False Recommendations', 'False Hierarchy', 'Price Comparison Prevention', 'Click Fatigue', 'False Limited Time Message', 'False Low Stock Message'

[80] The Consumer Protection in Electronic Commerce Act, 2012 art. 21.
[81] 'Recent Developments in KTFC's Efforts to Regulate Dark Patterns' (*KIM & CHANG*, 6 July 2023) <https://www.kimchang.com/en/insights/detail.kc?sch_section=4&idx=27534> accessed 5 January 2024.
[82] 'Update on the Regulatory Trends on Dark Patterns' (*SHIN & KIM*, 23 August 2023) <https://www.shinkim.com/eng/media/newsletter/pdf/2194> accessed 8 January 2024.
[83] Personal Information Privacy Act, 2011 (SK).
[84] *Update on the Regulatory Trends on Dark Patterns* (n 82).
[85] Korean Fair Trade Commission, *Guidelines on the Voluntary Management of Online Dark Patterns*, (31 July, 2023) (SK).

and 'False Activity Messages' being the unique ones.To tackle patterns like 'False Discount Claims' and 'False Recommendations', the guidelines provide that the consumers should not be given misleading information about standard prices, sales prices and discounts; the platforms should not (i) delete unfavourable consumer feedback or manipulate such feedback to conceal unfavourable feedback, and (ii) write false and manipulated positive reviews.

'False Hierarchy' employs graphic designs to trick users into thinking that they have no choice but to choose a certain option, and to prevent such UI/UX design, the guidelines suggest setting up a web page with options and alternatives available for consumers and arranging the options in a symmetric and like manner, for example, the "Cancellation tab" in a window should not be made in grey text giving the impression that consumers do not have the option to cancel. This tactic is quite common for windows requiring consent of the consumer in collecting their personal data such as cookie consent notices, a visual example of such pattern has been provided above in the paper (Figure 3).

'Price Comparison Prevention' as the name implies, makes it challenging for consumers to compare product prices online. While online platforms are not accountable for obstructions caused in comparison, they need to make sure to design an interface which does not provide inaccurate information of prices or any such detail which makes comparison difficult. 'Click Fatigue' basically works to tire consumers into giving up on making a choice which shall be beneficial for them.

'**False Limited Time Message**' misleads consumers into believing that the discounted price is only available for a short period of time which pressures them into buying the product, this pattern is a lot similar to 'false urgency' with a slight difference being its focus on time bound availability of discounted prices only. 'False Activity Messages' display the number of people who have recently viewed or bought a certain product, which pressures the consumer into purchasing that product as well.

The Korean guidelines have been one of the most comprehensive and illustrative guidelines on the subject so far, with the identification and enforcement against various dark patterns and proposed amendments under not only the E-Commerce Act but also the PIPA. While the Indian guidelines are somewhat at par with the Korean guidelines, the one place where Indian guidelines have more ground to cover is the interconnection between dark patterns and personal data protection and recognition of dark patterns as a threat to privacy of consumers

Argentina

Argentina, though, doesn't have a full encompassing law on Dark Patterns, it has passed some laws or decrees in the past few years to curb such practices. The laws concerning consumer protection

are the Argentine Constitution,[86] the Consumer Protection Law 24,240[87] as amended (CPL) alongside Regulatory decree no. 1798/1994;[88] the National Civil and Commercial Code (CCCN-Title III Chapter 1 "Consumer Contracts");[89] Decree 274/2019, concerning Unfair Trade and Competition practices.[90] Further, there are regulations of national, provincial and municipal level, as well as international treaties which Argentina adheres to. The definition of consumer in Argentinian law is very wide. Law 24,240 (art.1) and CCCN (art. 1092) defines 'consumer or user' as "the human or legal person who acquires or uses, for free or onerous, goods or services as the final recipient, for their own benefit or that of their family or social group." From the definition, it is clear that people who obtain or use goods or services-free of charge or for a fee-as the ultimate recipient for their own benefit or for the benefit of their family or social group-without becoming involved in the consumer relationship as a result of or on the occasion of it are also regarded as consumers or users.[91] All entities, or suppliers, or vendors that engage in a consumer relationship as a result of their operations must comply with the requirements imposed by the Consumer Protection framework. Argentina through its resolution 994/2021[92] forbid some deceptive practices which fall under Dark Patterns, such as 'sneak into the basket' or 'presume consent when consumers navigate supplier's websites to limit consumer's right of withdrawal' or 'obstruct, denature or limit the revocation of acceptance by consumers in consumer relationships carried out outside commercial establishments, remotely or by electronic means'. Some other striking feature of this legislation is that it also seeks to prevent Platforms or sellers from imposing a ban or sanction for making negative reviews,[93] or letting suppliers have consumer data available after the termination of the contract when the consumer has requested its deletion.[94]

Resolution 424/2020 passed by the Secretariat of Domestic Trade,[95] Argentina establishes that service providers and online retailers are required to prominently display and make easily accessible a link, that allows customers to cancel their orders for products or services. Consumers cannot be required to do any prior registration or any other procedure, as stated in Section 34 of Law No. 24,240[96] and Section 1110 of the Civil and Commercial Code.[97] The legislation even provided where to put the 'Withdrawal' or 'Cancellation' button, particularly in a prominent place in terms of visibility and size with the denomination indicated in the resolution[98]. This again can be an extension of laws introduced by various jurisdictions to make the option to cancel a good or service more convenient and accessible for consumers as hiding the 'Cancellation button' is one of the most prominent forms of dark patterns. Furthermore, the Mercosur Resolution No. 37 for 'Consumer Protection in E-commerce',[99] which mandates that e-commerce entities provide

[86] Constitution, art. 42 (Arg).
[87] Consumer Protection Law No. 24240 of 1993 (Arg).
[88] SECRETARÍA DE COMERCIO INTERIOR Resolución 1798/1994 (Arg).
[89] Civil and Commercial Code of the Argentine Republic, 2014 (Arg).
[90] SECRETARÍA DE COMERCIO INTERIOR Resolución 274/2019 (Arg).
[91] 'Consumer Protection Laws and Regulations Argentina 2023-2024' (*ICLG.com,* 28 April 2023) <https://iclg.com/practice-areas/consumer-protection-laws-and-regulations/argentina> accessed 19 January 2024.
[92] SECRETARÍA DE COMERCIO INTERIOR Resolución 994/2021, art. 1 (Arg).
[93] ibid art. 1(r).
[94] ibid art. 1(p).
[95] SECRETARÍA DE COMERCIO INTERIOR Resolución 424/2020 (Arg).
[96] *Consumer Protection Law* (n 87) s 34.
[97] *Civil and Commercial Code* (n 89) s 1110.
[98] 'The new Cancelation Link' (*Dentons,* 8 October 2020) <https://www.dentons.com/en/insights/articles/2020/october/8/the-new-cancelation-link> accessed 19 January 19, 2024.
[99] Mercosur/GMC/Res. No. 37/19 on Consumer Protection in E-commerce.

consumers with a 'clear, sufficient, truthful, and easily accessible way' to obtain information about the supplier of the good or service and the transaction made, is incorporated into the Argentinean legal system by the Secretariat's Resolution 270/2020.[100] Thus, transparency and minimum interference in the interface along with easy access to relevant information of the sellers is at the foundation of such laws.

Dark Patterns regulations in Argentina are still not very comprehensive or specific, but the regulations do try to alleviate some issues such as 'sneak in basket' or option to 'Cancel or Withdraw' and promote transparency in e-commerce and user interface. This approach is very similar to the one taken by India in terms of curbing unfair trade practices through means of dark patterns. One striking feature of the Argentinean regulations is that they not only acknowledge dark patterns prevalent in online interface but they also intend to cover similar practices employed by sellers/vendors in brick-and-mortar stores, which has not been discussed or touched upon by other jurisdictions. Dark Patterns like 'false urgency' or 'coerced action' like forced registration or enrollment in services can very much happen in commercial outlets along with websites.

V. The Way Forward

While the Dark Patterns Regulation in India and abroad have been analyzed and compared in this paper, a running theme in all comparisons has been the lack of integration of Dark Pattern regulations with Personal Data Protection Laws in India. It has to be acknowledged that categorizing 'forced action' as a Dark Pattern does fall within the purview of the Digital Personal Data Protection Act, 2023 ("DPDP"), but considering the necessity of protection of personal data in today's highly digitalized world, and the technical nature of the issue, more importance needs to be given to details to make the regulations all encompassing. Mere mention or statement of such a provision in the guideline still leaves room for misuse and illegal gathering of Personal data and hindrance on Privacy of Indian users. Consent has been made an absolute essential while giving away Personal data in the DPDP, with the caveat that such consent shall be "free, specific, informed, unconditional and unambiguous with a clear affirmative action".[101] But dark patterns strike at the very root of consent as it employs deceptive tactics for obtaining such consent, vitiating it as a result. Hence, the need for the Indian Regulator is to draw a clear link between dark patterns and their effect on consent received while sharing data to ensure the 'Right to Privacy' to each and every consumer.

A more helpful approach would be establishing a nexus or a link between the Data Protection Board, which has been equipped to deal with Data Protection in India, with the CCPA when it comes to dealing with cases which require specialized knowledge on data privacy, dark patterns and unfavourable trade practices by platforms online, this is because dark patterns and protection of personal data cannot be seen in isolation. Oftentimes, these dark patterns are shrouded attempts to

[100] SECRETARÍA DE COMERCIO INTERIOR Resolución 270/2020 (Arg).
[101] The Digital Personal Data Protection Act 2023, s 6.

gain personal data for selling or other profit-making ventures without the consent of the users. Monetization of personal data also causes a confluence of Data Privacy and Consumer Protection, which should be adequately addressed by either the Data Protection Board through Data Protection Rules or the CCPA in future for adequate safety and promotion of a consumer-friendly ecosystem in the digital space.

VI. Conclusion

These regulations have been a welcome step in the digital market ecosystem in India for bringing light to such concerning issues. The first step in regulating any unethical practice is to form a comprehensive framework to tackle it and bring some sort of clarity on the subject. These regulations do exactly that. It serves an important tool in highlighting such deceptive practices and making consumers aware of their rights. As discussed previously in this paper, implementation of guidelines on the subject of dark patterns is of extreme importance since such designs, on the face value, do not strike as irregular or illegal because of how they have been normalized in the UI/UX of websites. Every internet user in today's day and age has come across a dark pattern at least once while surfing on websites. Users have been tricked or misled into performing activities which do not benefit them but instead benefit the platform owners. These activities range from purchasing goods or services or disclosing personal information. Dark patterns have influenced all such activities.

The lawmakers by way of such regulations have attempted to establish more accountability and transparency on the part of online platforms and data providers, one of the major stakeholders, for the benefit of another major stakeholder- the consumers. A running theme in dark pattern laws and guidelines across jurisdictions, whether in India or South Korea or European Union, has been the importance accorded to consumer choice and autonomy and the right to make free and informed decisions. Free, unbiased consent and clarity in action in online activities is one of the intended consequences of such regulations which strike at concealed unfair trade practices in User Interfaces. Any pattern which subverts user autonomy shall attract such provisions, although the liability of a provider may or may not depend upon the 'intention to mislead' depending upon jurisdictions.

But from the comparisons drawn in this article, it can be inferred that these measures still fall short of being fail-safe in certain aspects such as data privacy. They attempt to regulate the rampant usage of Dark patterns by online platforms to coerce or psychologically trick consumers into making unintended purchases of goods and services but they remain silent on the role of such patterns in surreptitiously collecting personal data of users, often without their consent. Consent, if any, is vitiated by the lack of it being 'informed' and 'unambiguous.' There is a huge intersection of privacy laws and dark patterns, acknowledging such intersection contributes to greater protection of consumers in the online space. India is globally at par when it comes to regulations on dark patterns. In fact, it is even more comprehensive than some, but what these regulations require is a stringent

framework for their execution and a conducive space for consumers to understand such deceptions and enforce their rights for such regulations to be fruitful. Considering the fact that both the Data Protection Laws and Dark Pattern regulations are in their nascent stage around the world, it is yet to be seen how helpful these rules turn out in curbing dark patterns and other such ancillary unfair trade practices in the online space. The change that they will bring in the digital ecosystem is yet to be seen and gauged.

Exhaustion And Parallel Imports: US Vs. EU Perspective

DR. RAMNEEK KAUR

Dr. Ramneek Kaur is an assistant professor of law at Amity Law School, Mohali, Punjab

Abstract

The doctrine of exhaustion and the concept of parallel imports have long been subjects of contention in intellectual property law, with varying approaches adopted across jurisdictions. The Trade-Related Aspects of Intellectual Property Rights (TRIPS) Agreement provides member states with the flexibility to define the scope of exhaustion, leading to divergent national and regional policies. In the United States, a national exhaustion regime prevails, emphasizing the territoriality principle, thereby limiting parallel imports unless authorized by the intellectual property holder. Courts have consistently upheld this stance, allowing restrictions based on material differences that could mislead consumers and harm trademark owners. Conversely, the European Union embraces a policy of regional exhaustion, permitting the free movement of goods within the European Economic Area (EEA) while restricting imports from outside its borders. The European Court of Justice has played a pivotal role in shaping the doctrine, balancing the need for market integration with the rights of patent and trademark holders. Despite the flexibility offered by TRIPS, the global regulatory landscape remains fragmented. A harmonized international framework is needed to prevent conflicts and ensure that parallel imports are not unjustly perceived as an **u**

> *"Intellectual property, more than ever, is a line drawn around information, which asserts that despite having been set loose in the world - and having, inevitably, been created out of an individual's relationship with the world - that information retains some connection with its author that allows that person some control over how it is replicated and used."*[1]
>
> **`Nick Harkaway**

I. Introduction

In the realm of intellectual property rights, it is imperative to delve into the intricacies of the international facets surrounding the Doctrine of Exhaustion and the nuanced concept of Parallel Imports. These aspects manifest themselves distinctly on a global stage, influencing the extent

[1] Nick Harkaway, *The Blind Giant: Being Human In A Digital World* 131 (John Murray, London, 2012).

of assertion of control by the rights holders over their creations, and concurrently, how parallel imports can navigate the complex legal landscapes of various jurisdictions. A comprehensive exploration of these phenomena necessitates a deep understanding of the nuanced legal approaches to exhaustion doctrine and the complex web of parallel import considerations at the international front. Trade-Related Aspects of Intellectual Property Rights (TRIPS) Agreement finds a mention of principle of exhaustion thereby providing a flexibility to the member states in determining the scope and extent 'exhaustion'. In this chapter, the researcher would be discussing how provisions of TRIPS Agreement deal with the concepts of parallel imports and doctrine of exhaustion and the way they are dealt under the US law and the EU law.

II. Parallel Importation, Exhaustion and Trips Agreement

By virtue of the Trade-Related Aspects of Intellectual Property Rights (TRIPS) Agreement, Member States can flexibly determine the scope and extent of exhaustion they intend to follow. Every patentee under Article 28 of TRIPS has been entitled to have the absolute right of making, selling, offering for sale, using or importing the impugned patented product or process. However, a small caveat has been added to the exclusive right to import by footnote (6) to Article 28 which clarifies that the right of importation of goods is subject to Article 6.

Article 6 in this context provides that exhaustion of rights related to intellectual property shall not be addressed by anything in the TRIPS Agreement. Article 5(d) of the Doha Declaration further clarifies the meaning of Article 6 by providing that each member has the liberty to make their own system for exhaustion of intellectual property rights without interference as an effect of TRIPS.

The member countries under TRIPS are, therefore, clearly permitted to limit the exclusive right to import granted to them under Article 28 to such an extent that the said limitation in some way relates to the concept of 'exhaustion'.[2] Before discussing more on these provisions, it is important to discuss the situation that existed before TRIPS.

i. <u>Situation pre-TRIPS:</u> Before the negotiation of TRIPS Agreement took place, governments of different countries adopted various policies and regulations for exhaustion of intellectual property.[3] The Supreme Court of United States interpreted domestic law to establish a "common control"[4] when addressing the theory of exhaustion in trademark cases, the Court had never specifically addressed the issue of parallel importation in the area of patents.[5] Contrary thereto, there have been certain important decisions in favour of international exhaustion of patents by Court of Appeals.[6] Recognizing that if trademark holders were able to impede free movement of goods, the goal of European market integration would be preserved, the European Court of Justice (ECJ) pioneered the question of exhaustion and at an early stage invoked

---

2 Shamnad Basheer *et.al.*, "'Exhausting' Patent Rights in India: Parallel Imports and TRIPS Compliance", 13 *Journal of Intellectual Property Rights* 486 (2008).
3 *Adams* v. *Burke* U.S. (17 Wall) 453 (1873).
4 *Kmart* v. *Cartier*, 486 U.S. 281 (1988).
5 *Boesch* v. *Graff* 133 U.S. 697 (1890).
6 *Curtiss Aeroplane & Motor Corp.* v. *United Aircraft Engineering Corp.,* 266 F. 71 (2d Cir. 1920).

principles of competition law to preclude such action. Subsequently, however, European Court of Justice (ECJ) fashioned an "intra-Community exhaustion doctrine" to frame its jurisprudence on the subject. Other countries and regions also considered different regimes of exhaustion for protection of intellectual property rights. Countries of Latin America seemed majorly in favour international exhaustion, while Switzerland and Japan, respectively, had substantial jurisprudence on the issue. [7] Dr. Cottier, Member of the Swiss negotiating team at the GATT Uruguay Round from 1986-1993, opined that from a trade-related perspective, neither national nor international exhaustion are fully adequate; and from customer's perspective, regional or national exhaustion are not acceptable. Cheaper parallel imports may be prohibited, if it permits significant market segmentation and differential pricing strategies. However, from the rights holder's perspective, international exhaustion is insufficient.[8]

ii. <u>Introduction of TRIPS</u>: After arrival of TRIPS, the Doha Declaration read with TRIPS Agreement permit each Member to frame their own exhaustion regime freely without any challenge.[9] Article 6 of the TRIPS Agreement indicates that any desire to restrict Member state flexibility to regulate the issue of right exhaustion for all forms of intellectual property rights is not intended. This renders Article 6 highly pertinent for Member states as they integrate the concept of right exhaustion into their national legislation, irrespective of its scope on a national, regional, or global level.[10] Article 6 holds significance as it aids in interpreting the range and magnitude of exclusive rights conferred under different sections of the TRIPS Agreement. Lawmakers of various WTO members could be reluctant to enact exhaustion provisions at the national or international level for the want Article 6. The provision grants flexibility to the Member countries to determine the scope and the extent of exhaustion by specifying that no complaint would be heard in this regard.[11]

iii. <u>Exhaustion under realm of the TRIPS Agreement:</u> As seen, the focal point of parallel imports wrangle has been the TRIPS Agreement even before its inception in 1993. However, what TRIPS exactly provides in this respect is that subject to Articles 3 and 4, nothing in TRIPS shall be used for addressing exhaustion of rights associated with intellectual property. The provision is "neutral" since it does not impose any exhaustion regime (regardless of it being national, international or regional), and leaves it to the countries to adopt a regime that is most suitable as per their needs. It further clarifies that, regardless of the regime chosen, an immunity from legal actions is guaranteed before WTO courts. In other words, basically, Article 6 amounts to an 'agreement to disagree'.[12]

---

7 Frederick M. Abbott, "First Report (Final) to the Committee on International Trade Law of the International Law Association on the Subject of Parallel Importation", 1(4) *Journal of International Economic Law* 607 (1998).

8 Thomas Cottier, "The Value and Effects of Protecting Intellectual Property Rights within the World Trade Organization", 13 *Association Littéraire et Artistique Internationale* 22 (1994).

9 The Doha Declaration on the TRIPS Agreement and Public Health, *available at,* http://www.who.int/medicines/areas/policy/doha_declaration/en/index.html (Visited on July 20, 2024).

10 Carlos M. Correa, Trade Related Aspects of Intellectual Property Rights: A Commentary on the TRIPS Agreement 182 (*Oxford University Press*, Oxford, 2007).

11 Rajnish K. Rai, "Does India needs to harmonize the law of patent exhaustion and parallel imports?" 19 *Information and Communications Technology Law* 115 (2010).

12 Frederick Abbott, *et. al., The International Intellectual Property System- Commentary and Materials* 1797 (Kluwer Law International, The Hague, London, Boston, 1999).

In this regard, Doha Declaration on the TRIPS Agreement and Public Health, under Paragraph 5(d) provides that the outcome of the provisions of TRIPS relating to exhaustion of intellectual property rights, is to let each member free, without challenge, to form its own regime of exhaustion.

During the formulation of TRIPS Agreement, no compromise or consensus was arrived at amongst the member nations in respect of the principle of exhaustion and so eventually the final Agreement left the said issue unresolved. However, this issue per se has not been ignored under TRIPS but the Member countries are given the liberty to decide for themselves as to what principle of exhaustion they would want to follow.[13] A perusal of Article 6 makes is explicit that the issue of exhaustion of intellectual property was considered, however, no consensus or compromise could be arrived at and therefore, each member country was left to have its own laws for regulating the exhaustion of intellectual property.

The consequence of Article 6 is revealed in the text of Article 28 of TRIPS which specifies the minimum rights which are to be conferred on holders of intellectual property in Member states. The traditional rights against unauthorized third parties preventing them to make, to use, to offer for sale or to sell goods under intellectual property protection includes an expressly granted right to prevent unauthorized import of such goods. By virtue of Article 6, since each Member has been left free to decide on the principle both national and international exhaustion, they are also left to decide on its own accord whether or not to recognize exhaustion of the right of importation.

a. ***Studies of Parallel Imports under TRIPS:*** TRIPS rather than determining the issue of exhaustion of rights pertaining to intellectual property merely acknowledges that the issue shall not be considered for dispute settlement. In fact, in 1995, shortly after the TRIPS Agreement was concluded, the International Trade Law Committee (ITLC) of the International Law Association (ILA) got together for discussing the issues relating to the implementation of the TRIPS Agreement and a study to understand the job of parallel imports in the trading system internationally was also started. The schedule of ITLC for presenting its recommendations seemed to be set on the premise that a further amendment to the TRIPS Agreement was likely to happen in the year 2000, whereby possibly Article 6 would have been deleted. Apparently concerned by the possibility that removal of Article 6 would permit the national laws of member states opposing parallel imports to regulate trade sanctions against nations having laws permitting parallel imports, a direct examination of the merits of an affirmative policy favoring international exhaustion was undertaken as against the presently passive position of permitting parallel importation as a part of national policy. ITLC in its deliberations, appeared to have reached a conclusion that an affirmative policy that favors parallel imports should be adopted as a part of international trade policy. Committee on International Trade Law of the International Law Association in their Report on Parallel Importation came out with the said conclusion. The report was authored by an

[13] Frederick M. Abbott, "Parallel Importation: Economic and social welfare dimensions" *International Institute for Sustainable Development* (2007) *available at* https://www.iisd.org/system/files/publications/parallel_importation.pdf (Visited on 16 June, 2024).

ITLC Rapporteur Professor Frederick M. Abbot, and was released for comment in April 1997.

b. ***The Abbott Report:*** Three precepts formed the foundation for the purpose of analyzing the Report: (1) the basic principles of the WTO (2) underlying policies of intellectual property right protections and (3) the economics of parallel importation.[14] The basic principle of the WTO was simply stated as prohibition of tariff and all other barriers to the movement of goods and services within and across Member boundaries. So prohibition in respect to parallel importation clearly becomes a non-tariff barrier to international trade. There could be room for extensive debate regarding how appropriate such statements are, without qualification, as the underlying precept of the WTO. The discussion on parallel import, thus, could be undertaken while focusing on the remaining two principles.[15]

For the second cornerstone of the Report, it was proposed that the regarding the underlying ideologies of intellectual property rights, return of a reward to the owner in copyrights and patents while an additional protection in trademarks could help solve the issue. So far as patents are concerned, the purpose of the giving exclusivity is to promote innovation by granting a monetary reward to the inventor or owner. Similar is the case for copyright though directed to economic and moral support of the artists. For trademarks, an identification of origin, alongwith protection of consumers as well as the accumulation and preservation of goodwill, serves as an incentive for these rights. Such understanding formed the basis on which the Report was drawn underlying that once a reward is given to the intellectual property right owner, by way of profit or royalty, the bargain with all granting authorities is satisfied with no further obligation remaining. The Report's treatment towards intellectual property rights, for example, patents, does not consider expressly certain fundamental and unique attributes of such proprietary right. Though the Report has noted that as a basic principle, the patent rights are inherently territorial, there is no closer scrutiny, however, of the nature of such rights as they would exist worldwide for any given product. Even for the same basic development which happens in patents worldwide, there could be differences in scope, numbers or types of patents granted from Member to Member. In the environment in which the businesses exists today, such rights might be subject to complex international ownership or licensing arrangements which provide for a distribution of the reward as per the expectation of the patentee or owner(s). The expectation of a reward that has been distributed appropriately among several markets might be reasonable while seeking a return on research and development investment based on international marketing. It is apparent that there exist significant differences in the policy and planning which underlie the marketing of products protected under intellectual property and unprotected or "common" products.[16]

---

14 *Supra* note 8.
15 *Ibid.*
16 *Id* at 615.

As regards the final point of the Report, the economics of parallel importation have been considered while viewing it in basic manner as a matter of balance between consumer's interest and producer's interest. Certain important criteria for consumers are given priority such as price, quality, variety and service/product support, as well as the ultimate efficiency and effectiveness in providing goods and services world-wide to satisfy the demand. The seller's interest in a profit, as per the Report, should be satisfied by the first sale solely.[17] The economic consideration that was finally offered to justify an exhaustion of the intellectual property rights, even if at the price of the profitability of a market which had been established and is serviced by the producer, was that such policy would result in a desirable redistribution of wealth.Perceiving the issue of exhaustion as an extension of a regional or domestic issue to an international scale, the Report as regards patents notes that vertical territorial restraints would be permitted under existing national anti-trust laws. However, first sale doctrine provides an important policing function that causes the right of intellectual property to be exhausted on the receipt of compensation by the producer. So, while concluding, the Report mentions that the same principle that is embraced by both individual countries (like USA) and the regional groups (like the European Union) should be applied on the international scale. The Report, in this regard, however, minimizes several critical differences between the single and homogenous market which exists in individual nations and even economically united regions, as well as the complex multi-faceted markets which are present in the developed, developing and underdeveloped Members of the WTO. A regional group like the EU also has undisputed characteristics which clearly distinguish organization from the WTO while justifying their current policy regarding parallel imports in and out of the EU. In contrast to this, WTO does not possess any unifying characteristics or goals which would justify an affirmative parallel import policy, as well as existence of defined regulatory and structural goals, a commitment to free movement of capital and people, an express industrial policy for research and development, a defined competition policy, a monetary union, and common political goals.[18] Though the Report raises some interesting arguments, further analysis, research and development from a legal view-point (such as the achievement of a world-wide patent) would be necessary prior to an affirmative parallel imports policy even being ripe for debate. Also, the adverse effect of parallel imports on both developed as well as developing Member states cannot be simply brushed aside. Corporate Bodies in developed countries will certainly have their existing complex production and distribution arrangements damaged extensively, and their flexibility to create such arrangements as well as ensure that an expected return is obtained impaired severely. This could lead to an erosion of profit as well as a reduction in the capital available for essential investment on research and development. In respect of developing nations, there are strong chances that prices would be raised domestically because of increased

[17] *Id* at 612.
[18] *Id* at 618.

international competition, and additionally the sales of critical products could be terminated as well. The possibility of reduction in capital investment can not be ignored.

c. ***Resultant Article 6***: A compromise amongst nations supporting international exhaustion regime and parallel imports (generally developing and least developed nations) and nations supporting national exhaustion regimes (generally developed nations) on the other hand. However, some rich countries like Australia and New Zealand, which are net importers of products under intellectual property rights protection also supported an international exhaustion regime during the negotiations of Uruguay Round.[19] While on the other hand, most developing as well as least developed countries consider parallel imports as a tool to promote competition in foreign markets that prevents possible anti-competitive behaviours of intellectual property rights holders, and also as a good opportunity for economic growth.[20] Resultantly, international exhaustion regime is preferred by some of these countries have adopted.

III. Position in USA

Around mid-80's, parallel imports started gaining recognition in USA, when such imports resulted in trade worth 2-3% of whole imports in USA[21]. The neutral wording of Article 6 was adopted by United States allowing it to put pressure on as well as induce other countries for adopting methods to forbid or limit parallel imports. Such an act was permissible because TRIPS had set minimum standards of protection, leaving it onto the countries to freely adopt a method best suited for implementing the said protection.[22] This prompted countries like United States to enter into bilateral and regional contracts with other Members with an intent to obtain stronger intellectual rights protection. Bilateral free trade agreements were signed between United States and Morocco and Australia in the year 2004, respectively, for limiting parallel trade. Such accords, in particular, prevent parallel importation of products under patent protection, at least in situations when the holder of patent includes a territorial limitation by contract or other means with respect to how the products would be distributed.[23] The US-Singapore agreement entered into in the year 2003, contained a provision whereby parallel import of pharmaceutical products was limited, which gave a cause of action to drug companies against parallel importers that engaged in purchasing drugs from anyone they knew had been contractually prevented from selling to them. Such agreements formally comply with Article 1(1) of TRIPS that leaves members of WTO free to introduce stronger IPR protection. However, negotiating and concluding such agreements containing provisions as mentioned above, is not

---

19 C. Fink, *et.al* (eds.), *Intellectual Property and Development – Lessons from Recent Economic Research* 173 (World Bank and Oxford University Press, Washington, DC, 2005).

20 Surinder Kaur Verma, "Exhaustion of intellectual property rights and free trade: Article 6 of the TRIPS agreement" 29(5) *International Review of Intellectual Property and Competition Law* 534 (1998).

21 *Supra* note 22.

22 Article 1(1) TRIPS Agreement

23 E. Bonadio, "Parallel Imports in a Global Market: Should a Generalised International Exhaustion be the Next Step?" 33(3) *European Intellectual Property Review* 153 (2011).

consistent with the Doha Declaration's multilateral spirit, that permits countries to freely choose an exhaustion regime most suitable to their own needs in the best possible manner (without any pressure from other countries).[24] And generally, such a bilateral approach adopted by countries whereby they agree to be a segment of a multilateral context (the WTO) is considered as violating the international law obligations.[25]

The existing legislations and the court decisions (as discussed subsequently in the chapter) demonstrate that position in United States is that parallel imports are not allowed and exhaustion is limited to nationwide boundaries. Through its courts, the United States, has long held that it would not recognize intellectual property right exhaustion outside its boundaries.

i. Consideration under US Patent Law

The patent law in United States on parallel imports dates back to 1890. In Boesch v. Graff[26] a case where whether an American patent holder of lamp burners, the plaintiff, could be permitted to prevent the import of the said product from Germany by the defendants who had acquired the said product from a seller who was entitled to transact under a German prior user law, was in issue.[27] It was opined by the Court that an invention on getting a patent in the United States and in a foreign country, product containing the invention cannot be permitted to be imported without the patent holder's consent, regardless of the product having been purchased from an authorized seller in a country outside. The Court, thus, declined to permit exhaustion of patent rights since exhaustion was limited by nationwide boundaries.[28]

However, if a patent holder in USA sold a product under patent protection in a foreign country under circumstances which indicate absence of restrictions on resale, express or implied, the patent holder cannot prevent the person who buys the product from importing that product in the United States, either for use or resale.[29] Such a situation, could however be avoided by the holder by including a provision in the sales contract which prohibits importation back into USA.[30] Such a practice is also known as the modified international exhaustion. Until the year 2001, a rule establishing modified international exhaustion was being followed in the United States[31], accordingly, only subject to express contractual restrictions being entered into by the patent holder enforceable against the importer, parallel imports of products were allowed. It was recognized consistently that upholding of the exclusive right of the holder of the patent up to the point of first sale would provide adequate financial incentive to the patent holder to obtain the benefits of his creative invention.

---

[24] UNCTAD-ICTSD, *Resource Book on TRIPS and Development* 92 (Cambridge University Press, New York, 2005) *available at* https://unctad.org/system/files/official-document/ictsd2005d1_en.pdf (Visited on May 31, 2024).

[25] M. Ricolfi, "Interface between Intellectual Property and International Trade: Agreement on Trade Related Aspects of Intellectual Property Rights" *available at* https://www.ipmall.info/sites/default/files/hosted_resources/Teaching_IP/Marco_ Ricolfi_2001. pdf (Visited on June 12, 2024).

[26] 133 S. Ct. 697 (1890).

[27] Arghya Sengupta, "Parallel Imports in the Pharmaceutical Sector: Must India be More Liberal?" 12 *Journal of Intellectual Property Rights* 401 (2007).

[28] *Boesch* v. *Graff* 133 S. Ct. 697 (1890).

[29] *Holiday* v. *Matheson*, 24 F 185 (S.D.N.Y. 1885).

[30] *Coastland Corp.* v. *County of Currituck*, 734 F.2d 175 (4th Cir. 1984).

[31] Janice M. Mueller, *An Introduction to Patent Law* 364 (Aspen Publishers, New York, 2003).

In Curtiss Aeroplane and Motor Corp v. United Aircraft Engineering Corp[32], a suit for patent infringement, the plaintiff company was holding American and Canadian patents which related to certain kinds of aeroplanes that were licensed by the company to the British government for use during the World War-I. After termination of the war, the planes were sold by the British government to the defendant who imported the said planes to the United States for resale.[33] Challenging legality of the re-sale, it was questioned as to the point of time the intellectual property holder's rights would be exhausted. The Court opined that the moment the patent holder has sold the patented product, the same becomes freed from the patents contained therein. So, when the plaintiff sold the said planes to the British Government, the latter as the buyer obtained absolute rights to handle said planes in whichever way it desired. Since the defendant's rights accrued from the same and also since the said rights were without any restrictions as to alienability, it could not be prevented by the plaintiff from importing the said planes to the US for resale. The underlying logic behind the decision is that a sale of product under protection by the patent holder, out of his own desire, while choosing not to impose any restrictive condition, gives the buyer an absolute title to the product. Hence, the holder cannot prohibit future parallel imports of the goods since it was within his power to prohibit the same ab initio when it was being sold for the first time, and he voluntarily did not exercise this right. From the point of balancing competing interests as well, the Court opined that such a conclusion was justified since the patent holder's financial interests was protected by way of the monopoly he had over the products till there were sold for the first time which itself would be dependent upon a decision by him; also at the same time, trouble to the public by way of limited supply was prevented by not preventing parallel imports following the first sale having been executed.[34] The concept of exhaustion having been triggered through the sale of a patented product for the first time is premised on the belief that the patent holder through the sale has received adequate reward for his creative investments.[35] Thus, what is crucial is to make sure that the first sale was authorized by the patent holder.

The nuance, as discussed, in the law relating to exhaustion was delved into by the Supreme Court of US in the landmark case of Boesch v. Graff[36] wherein the Court opined that parallel imports could be prevented when the imports were in accordance with a prior user law, because the rights of the defendants emanated from the sale of the patented product made by the German seller who did not act under the authority of the US patent holder. So, the rights that were transferred to the defendant could not be extended to permit importing into the USA a product that was patented independently. Thus, the rationale of the decision is based on the fact that foreign sales by third parties, of products that are patented, with no relation to the patent holder cannot trigger exhaustion of his rights because such an opinion would be financially

---

32 266 F 271 (2d Cir 1920).
33 *Supra* note 30.
34 *Keeler* v. *Standard Folding Bed*, 157 US 659 (1895)
35 Margreth Barrett, "A Fond farewell to parallel imports of patented goods: The United States and the rule of international exhaustion", 24(12) *European Intellectual Property Review* (2002) 572.
36 *Supra* note 29.

detrimental to the patent holder as well as insufficient in compensating the patent holder for the expenses he incurred in creating the product itself.[37]

This modified international exhaustion approach, which was prevalent on the subject for over a century was overturned surprisingly by the Court of Appeals of the Federal Circuit in the case of Jazz Photo Corp v. International Trade Commission[38] that embodies the law in USA on the point. Plaintiffs, in this case, held patents in regard to a disposable camera that was not designed for reuse after its exposure of its film. However, certain Chinese refurbishers reused the shells of the camera which were later purchased by the defendants who supplied the films as well as imported these cameras into the markets in US.[39] The issue in the case was whether by refurbishing cameras that were patented in the USA and thereafter importing them from China, did the defendants infringe the rights of the plaintiff held by virtue of its patents. The Court opined that such parallel importation constituted infringement. It is pertinent to note that the Court on its own raised the issue of territoriality of exhaustion as well as proceeded to summarily reverse a catena of precedents that were accumulated over the past century.[40] Under laws in US, patent rights of a patent holder could not be exhausted by sales of a foreign provenance. The first sale necessarily had to be in US, for such exhaustion to occur. Thus, an import pursuant to a foreign sale of a patented product would still be capable of constituting an infringement under US patent laws. The only authority cited by the Court in support of its reasoning was Boesch v. Graff.[41] However, as mentioned, the case is not considered an authority for the proposition that as opposed to international, exhaustion must be territorial. On the contrary, it represents a decision which is fact specific, stating only that for the first sale to result in exhaustion of the patent holder's rights, the same ought to be authorized by the patent holder himself. This decision does not plainly translate into an inference that doctrine of exhaustion exempts all foreign sales.

So, a sudden and unexpected volte face was performed by judiciary in US to territorial exhaustion, by restricting the scope of parallel importation severely. The forum chosen by the Court for effecting such change was hardly pertinent as the matter of territoriality of exhaustion was not even in issue in the matter of Jazz Photo[42]. Also, the reasons provided by the Court for the moving away from international exhaustion were not satisfactory. Several hostile precedents were ignored and the ones that were relied upon too were distorted to construe inferences that did not flow naturally out of the decisions. So following a policy of territorial exhaustion in principle indicates a retrograde step in the development of jurisprudence of intellectual property in the context of world trade.[43] In a world that is increasingly unifying and where norms of protectionism are considered adversative, such decision supporting the cause of territorial exhaustion sticks out like a sore thumb as well as inhospitable with the global trend of free movement of products transcending geographical frontiers of nation states.[44]

---

37 *Ibid.*
38 264 F 3d 1094 (Fed Cir 2001).
39 122 S Ct 2644 (2002).
40 *Supra* note 30.
41 *Supra* note 29.
42 *Supra* note 41.
43 *Supra* note 38.
44 *Supra* note 30.

ii. Consideration under US Trademark Law

Much importance is given to territoriality of trademark under the trademark law in US. The trademark law in US propagates that the proper function of a trademark is not necessarily identification of the origin of a product, although it may do so, however, it is instead to denote the domestic goodwill of a domestic trademark holder for the purpose of letting the consumers rely on an expectation of consistency of the reputation earned by the holder for the trademark, and the holder of the trademark may believe that his reputation and goodwill will not be injured by use of the trademark by others in domestic commerce.[45] According to the US law, the ultimate concern for prohibition or regulation of parallel imports is analyzing factually if the customers of US have likelihood of confusion as to the origin of products from foreign manufacturers or exclusive importers of US. If the parallel imported products are recognized by the customers as exactly the products manufactured by a foreign manufacturer, imports will then not be blocked. But, if there is any confusion for the customer or the customer feels that the imported products have originated from the trademark owner in US, then it would block such parallel imports.[46] The regulatory mechanism adopted by US to legally regulate parallel imports is discussed hereunder:

Importation of goods bearing a trademark owned a US citizen and registered in the US Patents and Trademarks Office, is absolutely prohibited by Tariffs Act §526. There is no requirement of likelihood of confusion amongst the customers for such a ban on importation. However, Tariff Act cannot restrict imports of grey goods if there is an existing parent-subsidiary relationship between US distributor and foreign manufacturer.[47] However further, if an exclusive distributor happens to be the owner of a registered trademark in the US, independent of a foreign manufacturer, and has a separate goodwill in the product, then he would be entitled according to §526 to prevent imports of even genuine products that are obtained from the same foreign manufacturer.[48] The Tariffs Act, in its application, seems to be limited as it provides protection to those trademark holders who are citizens of US and form an entity different from a foreign manufacturer (i.e. under no parent-subsidiary relationship with the original manufacturer). As long as the products copy or simulate a trademark registered in the US, §42 of the Lanham Act provides that trademark owners would be allowed to prevent parallel imports of products, thereby overcoming the limitation. The provision highlights the principle of territoriality which is prevalent in the US, along with providing that as long as the customers are aware that the grey products are actually products that have not originated from the US manufacturer and are rather imported, parallel imports are permitted. Importation of genuine products is not barred but importation is barred only if the products simulate or copy a trademark.[49]

---

45 *Osawa & Co* v. *B&H Photo* 589 F.Supp 1163.
46 Sneha Jain, "Parallel Imports and Trademark Law", 14 *Journal of Intellectual Property Rights* 14 (2009).
47 *Yamaha Corporation of America* v. *ABC International Traders* 703 F.Supp. 1398.
48 *Premier Dental Production Company* v. *Darby Dental Supply Company* 794 F.2d 850.
49 *Olympus Corporation* v. United States 792 F.2d 315.

What actions would amount to copying or simulation is a matter that courts have to decide based on the peculiar facts of the case. In the case of Lever Brothers Co v. United States of America[50], the Court stipulated that foreign products that bear a trademark identical to a valid trademark of US but which is physically different, would be barred under § 42 regardless of the genuine character of the trademark abroad or affiliation between the producing entities.[51] In situations where trademarks which are though identical but have acquired different meanings in different countries, there is a likelihood of confusion to be created (in the absence of any specially differentiating feature) by the person who imports the foreign version to sell it under the trademark and such a likelihood of confusion is sought to be avoided through the Lanham Act.

So the provision in this regard apparently appears to be aiming at deceit and consumer confusion. Affiliation, a limitation under the Tariff Act, amongst the producers neither serve as a constructive consent to the importation nor in any manner reduce the probability of consumer confusion.[52] The Appellate Court, in appeal, upholding the decision of the District Court recognized the exception of affiliation[53] being inconsistent with §42 of Lanham Act that cannot be enforced as against foreign products that bear trademark identical to valid trademark in US though which are physically and materially different, as nothing in provision's administrative practice or legislative history supports such exception, and because physically different foreign products cannot be 'genuine.'[54] Hence, interpretations given to §42 in this case carved out an exception to the 'affiliate exception' for barring import of grey market products, with the test being that there were material and physical differences between the authorized products and the parallely imported products. A natural corollary that follows is that as long as the imported products are genuine, that is, they are identical or similar to the products which are authorized for importation by the trademark holder in US, parallel imports will be allowed. However, if the products are different, they will not be regarded as genuine and so importation would be liable to be barred. If one wants to claim protection under this rule laid down in the case, he would have to make an application to the Customs Authority alongwith a note of summary regarding the material and physical differences between the grey products and the products authorized by the trademark owner in US for importation or sale. If the entry of grey market products is prohibited by virtue of grant to the protection sought, such entry may still be permitted on assurance of the importer to properly label the products as per the Customs Regulations along with a notice.[55] The product or its packaging must carry the said labelling which needs to be conspicuous as well as legible. It should stay on the product till first sale to a retail customer in the US.[56] Hence, a parallel importer has only the following remedies available in case a suit for infringement if filed against him or if the grey market products are detained:

---

50 877 F.2d 101 (D.C. Cir. 1989).
51 *Supra* note 50.
52 *Lever Brothers Co* v. *United States of America* 877 F.2d 101 (D.C. Cir. 1989).
53 Customs Regulation §133.
54 *Supra* note 56.
55 Customs Regulations 133.23(b)
56 *Ibid.*

prove either that the products are not materially and physically different from the products authorized by the trademark owner in US; or that he has followed rules for proper labelling to ensure that customers would not get confused as regards the origin or source of the products.

a. ***Material Differences Test***: This test helps in determining whether there is a likelihood of injury that can be caused by the allegedly infringing products to the goodwill built in the trademarked products by the trademark holder.[57] When the alleged infringer and the trademark holder use identical marks for their products but the products are materially different, there is a likelihood of confusion amongst the consumers regarding the nature and quality of the trademarked products.[58] If the products of the alleged infringer do not share the characteristics of the products of the trademark holder, the perceptions of the consumers is likely to be affected regarding the desirability of the products of the trademark holder.[59] Sales of products of the alleged infringer would injure the trademark owner by tarnishing the 'commercial magnetism' of the trademark.[60] When such circumstances exist, the products of the alleged infringer are considered as 'non-genuine' and their sale would constitute infringement. On the contrary, if the differences between the products are proved to be so minimal that consumers while purchasing the alleged infringer's products "get precisely what they believed that they were purchasing", the perceptions of the consumers of products that are trademarked are not likely to be affected by sales of the alleged infringer.

   There is a possibility that the consumers could be unaware of the precise avenues travelled by the given product on its way to the shelf of a supermarket, however, presence of an authentic trademark on the product of the alleged infringer serves as an accurate indicator of its quality and nature. So in the case of Iberia Foods Corp v. Romeo[61], parallel importation of products was allowed because the plaintiff could not established any material differences. But in case where difference existed between the products that were imported parallely, prohibiting such imports, injunction was granted. On existence of significant differences between Italian made PERUGINA chocolate and the parallelly imported Venezuelan made PERUGINA chocolate, the Court opined that when a product which caters to the indigenous conditions of a foreign country while domestically competing against a product which is different physically but bears the same name, the potential for consumer confusion is extremely high. If there exists any difference in product of the trademark owner of US and the grey products of the alleged infringer so much so that consumers would be likely to consider it relevant when they would purchase a product, this aids in creating a presumption of consumer confusion which is sufficient to support a claim under the Lanham Act. Hence, the threshold of materiality needs to be kept so low that it is enough to take into account the potentially confusing differences that is, differences which are not enough

---

57 *Weil Ceramics & Glass Inc* v. *Dash*, 878 F.29 659 (3d. Cir. 1989).
58 *Societe Des Produits Nestle SA* v. *Casa Helvetia Inc*, 982 F.2d 633 (1st Cir. 1992).
59 *Martin's Herend Imports Inc et al.* v. *Diamond and Gem Trading Usa Co et al.* 112 F.3d. 1296 (5th Cir. 1997).
60 *Mishawaka Rubber & Woolen Mfg Co* v. *S S Kresge Co*. 316 U.S. 203 (1942).
61 150 F.3d 298 (3d. Cir. 1998).

blatant for the average customer to think obviously that the origin of the product is different from his expectations. Such a presumption can be overcome if the defendant offers a proof that the differences are not of such kind that on average, consumers purchasing the product are to likely consider them.

b. ***Quality Control Measures***: In the Iberia case[62], it was further argued that there existed material differences between the product sold by the defendant and the product sold by the plaintiff (Iberia) since Iberia conducted an inspection for 'quality control' of every shipment that had the impugned products on receipt from Caribe. It was contended by the plaintiff that the rejection of substandard goods has resulted in the raised the quality of the product (Mistolin) sold by the plaintiff thereby making it materially different from defendant's uninspected product (Mistolin). Placing reliance on the case of Casa Helvetia[63], the Court opined that on arrangement of the trademark owner to have its trademark placed on a product that has been manufactured by some other company, the rigorous quality control by the owner and inspection procedure once the products are received from the manufacturer are generally regarded as the criteria of checking material difference between products offered by the owner of the trademark and the products offered by the other company without stamp of approval of the trademark owner.

Though subtle differences in quality could be created by the quality control measures which are difficult to measure, however, important to consumers, hence, the trademark owners are not required by the Courts to demonstrate that the actual quality of the uninspected products is measurably lower than the products which are inspected.[64] But the test rather is to ascertain whether the procedures of quality control that have been established by the trademark holder are likely to highlight differences between the products so that consumer confusion as regards the source of the products could injure his goodwill.[65]

Customer Confusion as to Source or Origin: A cosmetics company of France along with selling its US operations to plaintiff, Bourjois, assigned its trademark JAVA, to them. The plaintiff continued to buy in bulk some cosmetic products from the French manufacturer which were later being sold by them in US in boxes that prominently displayed that the plaintiff is the importer. The boxes that the plaintiff was using were considerably similar to the boxes that were being used by their French predecessor manufacturers. Genuine cosmetic products were purchased directly from the French manufacturer by the defendant, being a third party, in the boxes used by them which the defendant later imported into the US. This made defendant's boxes similar to that of the plaintiffs.[66] Since during the 1920s, Courts were not inclined to protect trademark

---

62 *Iberia Foods Corp* v. *Romeo*, 150 F.3d 298 (3d. Cir. 1998).
63 *Supra* note 62.
64 *El Greco Leather Products Co.* v. *Shoe World Inc.* 806 F.2d 392 (2d Cir. 1986).
65 *Warner-Lambert Co* v. *Northside Dev Co.* 86 F.3d 3 (2d. Cir. 1996).
66 *A Bourjois & Co.* v. *Katzel*, 275 Fed. 539 (2d. Cir. 1921).

owners of US from imports of genuine products obtained from some foreign manufacturer, hence the defendant was allowed to sell the impugned cosmetic product imported by it from the manufacturer in France. It was argued in appeal that the impugned trademark belonged to a French house which truly indicated the origin of the products. However, Supreme Court opined that as a result of such import, confusion amongst the consumers as to the origin of the goods, was likely to occur. The Court applied the principle of territoriality and observed that by public understanding, the impugned trademark indicated that the products were coming from the plaintiff even though the plaintiff did not make them. Also, the sellers cannot be permitted to convey their products free from restrictions to which they themselves are subject. The Court opined that because the products had been effectively assigned to the plaintiff and the French manufacturer did not have any right to vend the products in US, defendant or any other buyer from the French company did not get any greater right to use.[67] This case has been considered as precedent and is applied by the Courts while deciding almost all cases of parallel imports.

For a brief period of time, uncertainty reigned in the US legislative around 1983 when in the case of Bell & Howell: Mamiya Co v. Masel Supply Company,[68] parallel imports of genuine cameras under a Japanese brand MAMIYA were allowed by the Court observing that little confusion would appear, if any, since it was not shown that the cameras which were parallely imported were inferior to the ones being sold by the plaintiff. Those parallel imports are barred under §42 of Lanham Act that involve products bearing a name or a mark that has been calculated for inducing the public into believing that a foreign product has been manufactured other than the actual country or locality, in some foreign country or locality. Therefore, making it mandatory to mark the imported products with 'country of origin', according to the labelling provisions of the Customs rules. The ruling in the case of Baldwin Bracelet Corp v. Federal Trade Commission[69] also made this essential. In this case, the plaintiff was directed to cease and desist from selling the impugned products which were packaged in a way that the purchaser was precluded from noticing the marking of foreign origin. A suit under §43(a) of Lanham Act may result if there is a failure to mark grey products with the country of origin.[70]

Supreme Court of US in the case of K-Mart Corp. v. Cartier Inc.[71] opined that a customs regulation that permits importation of products that are foreign made where the trademark owner of US has authorized the use of the trademark, it would be in conflict with §526 of the Tariff Act, 1930 which as per its plain language prohibits importation of any product of foreign manufacture that bears a trademark owned by a corporation

---

67 *Ibid.*
68 719 F.2d 42 (2d. Cir. 1983).
69 325 F.2d 1012 (D.C. Cir. 1963).
70 *Bonsei Enterprises Co.* v. *Porteons Fastener Co.* 441 F.Supp 162 (1977).
71 108 S. Ct. 1811 (1988).

or a citizen of US; as well as domiciled in the US. It was concluded by the court that the imports which are permitted by regulations from companies under "common control" are consistent with §526 and hence allowed. However, since exhaustion limited to within US, the Court refused to recognize exhaustion of trademark rights. In the case of United States v. Eighty-Three Rolex Watches[72], it was held by the Court that domestic trademark owners as well as foreign owned trademark owners are protected by §526, till the time the foreign owned trademark owner is not subject to the exception of "common control".

iii. Consideration under US Copyright Law

The long going battle regarding legality of parallel imports under the copyright law in US was resolved by the decision in Kirtsaeng v. John Wiley & Sons, Inc.[73]. A split of authorities existed on the issue prior to the decision- the Second Circuit opined that international exhaustion did not apply to copies manufactured outside of US;[74] on the contrary, the Ninth Circuit opined that international exhaustion did apply to copies manufactured outside of the US, however, only if they were first sold in the US,[75] and it was opined by the Third Circuit that a limitation of the doctrine of first sale to only such copies that were made within the US did not fit within the scheme of the Copyright law.[76] However, in Kirtsaeng[77], where it came to the notice of the alleged infringer, a citizen of Thailand attending graduate school in the US, that a discrepancy of significant nature existed between the prices of textbooks in US and in Thailand. Taking advantage of the price difference, he asked his family and friends in Thailand to buy copies of the cheaper foreign versions and send them to him which he could then sell online, and later reimburse his family and friends for the purchase as well as shipping costs, and thereafter keep the remaining profit for himself. John Wiley & Sons (Asia) Pvt Ltd had made and first sold abroad, a number of books among the ones imported and sold by alleged infringer. Such foreign textbooks generally stated that the book could not be imported into US and could only be sold in a particular country.[78] A suit was filed by Wiley for violation of its rights of importation as well as distribution, wherein it was argued by Kirtsaeng that first sale in Thailand exhausted such rights.

While the trial court as well as the appellate court both found infringement, however, the decision was reversed by the Supreme Court making it clear that international exhaustion was recognized.[79]

---

72 992 F.2d 508 (5th Cir. 1993).
73 2013 US LEXIS 2371 (2013).
74 *Kirtsaeng* v. *John Wiley & Sons, Inc.,* 654 F.3d 210, 213 (CA2 2011).
75 *Omega S. A.* v. *Costco Wholesale Corp.,* 541 F.3d 982, 986 (CA9 2008).
76 *Sebastian Int'l, Inc.* v. *Consumer Contacts (PTY) Ltd.,* 847 F.2d 1093, 1098 (CA3 1988).
77 *Kirtsaeng* v. *John Wiley & Sons, Inc.* 2013 US LEXIS 2371 (2013).
78 *Ibid.*
79 *Ibid*

In the case of Quality King v. L'anza Research International, Inc.[80] the Supreme Court of US opined that a copyright owner of US who sold copyrighted products in Europe at low prices could not be permitted to prevent such goods from being reimported into US. Though the issue of international exhaustion was not addressed by the Court expressly, the Court affirmed implicitly the propriety of laws which treat exhaustion as a matter for national determination solely.[81]

Though the Kirtsaeng case[82] settled the split of authority under Copyright Law of US, however, a conflict between patent law and copyright law was caused as regards the treatment of international exhaustion.[83]

IV. Consideration under European Union

Regional exhaustion boundaries have been enacted in European Union and the policy followed by European Union is not substantially different from policy followed by US. The European Union's policy of regional exhaustion is somewhat similar to the US policy of national exhaustion, since the member nations of the European Union are analogous to the individual states of US. Exhaustion is not recognized outside the region/states but within the region/states. Though each member nation of the European Union has its own intellectual property laws, however, the creation of the region of European Union has brought uniformity with it. Hence, unlike United States, in European Union, the need to promote market integration has colored the issue of exhaustion and parallel imports and so it has ceased to remain a debate that is purely confined within the parameters of intellectual property law.[84] There are varying conceptions of exhaustion as well as policy questions with respect to the permissibility of parallel imports in European Union. But it is far from a settled position. So, it would be premature to claim that the law relating to exhaustion in European Union has transcended the moniker of the ephemeral.

i. Considerations under the Patent Law

An independent jurisprudence has been spawned by European Court of Justice in respect of exhaustion of rights and parallel imports intending to harmonize the interests of integrated common market and that of the patent holder in enabling him to receive a fair return from the patent held by him.[85] In its effort, a compromise has been arrived at by the Court through which exhaustion of rights are deemed to occur at a community level though patent holder may continue to claim protection if he is able to show that he was under a legal obligation to market the products in a particular territory.[86]

---

80 1998 U.S. LEXIS 1606

81 Alan J. Kasper, "A View of the Parallel Imports Issue From an International Perspective", *available at* http://www.sughrue.com/files/Publication/51080ce5-5e07-415e-98eb-1ee3b141aca9/Presentation/PublicationAttachment/bb332de0-2005-48be-b0f4-1f5a991feabc/par_imports.htm (Visited on July 11, 2024).

82 *Supra* note 81.

83 Christopher J. Clugston, "International Exhaustion, Parallel Imports, and the Conflict between the Patent and Copyright Laws of the United States", 4(3) *Beijing Law Review* 95 (2013).

84 *Supra* note 30.

85 Thomas Hays, *Parallel Importation under European Union Law* 7 (Sweet and Maxwell, London, 2004).

86 *Merck and Co. Inc.* v. *Primecrown Ltd* and *Beecham Group Plc* v. *Europharm of Worthing Ltd.* [1997] 1 CMLR 83.

The first case before the ECJ which became a landmark in this regard was Centrafarm v. Sterling Drug[87] which provided the Court with an opportunity to define clearly the extent for which patent protection could be granted. The central issue in this case was whether the national patent law could be used in barring parallel imports without being foul of the principle of free movement of products. Using the principle of community exhaustion of rights the Court held that once the patent holder had consented to market the patented products anywhere in the common market then regardless of national patent rights that may exist, the product could be marketed and sold anywhere in the community. The decision was based on the rationale of the twin planks of patent holder's consent and the need for free movement of products. If the patent holder allows products to be marketed consensually, he cannot be permitted to retract such representation thereby later seeking to take recourse to national laws for prevention of parallel imports. Permitting the patent holder to do so would be akin to partitioning national markets which would be abhorrence of the principle of free movement that underlies the entire existence of the European Union. However, the Court recognized that if principle of free movement as enshrined under Articles 28 and 29 was to be derogated on the grounds of protection of intellectual property; it could only be permitted to be done if it justifies to safeguard the rights constituting the specific subject matter of that intellectual property which is the prerogative of the intellectual property owner to reap the benefits of the first sale of the product. Hence, where the said prerogative had to be protected, not as a matter of principle, national laws could only prevent parallel imports. The Court in the present case did not regard that this exception clause was satisfied, however, the rights of the patent holder were considered exhausted once products were marketed anywhere in the community with his consent.

In another case Merck & Co Inc v. Stephar BV[88] the question was: in case pharmaceutical products are marketed in a country where there does not exist any patent protection for the same, would it lead to exhaustion of the rights of the intellectual property owner. The Court opined that derogation from the principle of free movement of goods while effectively preventing partitioning of national markets could be allowed only when such derogation is essential in protecting the subject matter of the intellectual property right. It was observed that the rationale of recognizing this right is to ensure that the inventor is rewarded for his creation while also incentivizing analogous future inventions. Thus, if the patent holder markets his invention consensually in any country within a community, the inference that can be drawn is that either he has received some reward for his invention or he has unilaterally waived his right for the same. Such is so because the decision to place a product for marketing in a community as well as the conditions under which the product is to be marketed are sovereign decisions of the patent holder. On such decision being made, the patent holder must also be deemed to be willingly have accepted the consequences of his action. He cannot, at a later time, take recourse to national law for prevention of import of products from another state where he himself had lawfully marketed the said products. Thus decision of the Court even in this case was based on

[87] Case 15-74, decided on 31 October 1974.
[88] ECR [1981] 2063.

the issue of consent of the patent holder in marketing his products in member states where no patent protection existed. In the opinion of the Court, no material difference existed in the two cases: in one case where a genuine parallel patent existed and the other case where product was marketed in a country where patent protection did not exist; because as per the Court, in both the cases an independent conscious decision had been made by the patent holder. Because the nature of the decision was such, the Court opined that in both cases, the rationale for the grant of a patent that is, conferring of a reward on the patent holder through first sale had been satisfied. If the principle of exhaustion was deferred in any manner, it would lead to twisting of national markets thereby adversely affecting consumer's access to products in different markets. As a consequence once the products are marketed with the consent of the patent holder anywhere within the community, his rights would be exhausted and parallel imports would be permitted regardless of the prejudice that may be caused to the patent holder.

The law on the issue of parallel imports in pharmaceutical products in Europe was laid down by the case of Merck and Co. Inc. v. Primecrown Ltd.[89] The issues in this case were whether an exception could be carved out to the principle of community exhaustion for cases where products (drugs) are manufactured in countries they could not be patented, as a result prevent parallel imports; as well as in the specific situations where patent holders are under an ethical or legal obligation to put certain products on the market, whether the protection granted to the patent can act as a shield to repel parallel import. It was opined by the Court that a patent holder who, with full knowledge that no patent protection was available in a country, had willingly placed his products on the market therein, had exhausted his rights to control any subsequent circulation of such products in the common market. It would be an irrelevant consideration as to which country was the drug marketed in because the cornerstone for determining the point at which the rights are said to be exhausted is the consent of the patent holder in marketing the product. However, in cases where the patent holder is under a genuine legal obligation to market products in a particular country, presumption as to such consent cannot be made and the patent protection would continue.[90] Otherwise, in every other case, consensual marketing would presuppose that the rationale of deriving a benefit, in the form of reward, from the patent had been satisfied and so permitting a free circulation of products henceforth would not be an abhorrence for the underlying basis of providing intellectual property protection.[91]

Hence, an inference can be drawn from the aforesaid decisions that in its endeavour to balance rewarding inventor's creative efforts by providing appropriate returns by granting patent protection and the interests of market integration, the Courts in Europe have leaned towards the latter.

ii. Considerations under the Copyright Law

---

89 [1997] 1 CMLR 83.
90 Fiona Schaeffer *et.al.*, "Parallel imports of pharmaceutical products: A new realism, or back to basics", 18(3) *European Competition Law Review* 137 (1997).
91 *Supra* note 30.

The principle of exhaustion of copyright was applied for the first time by the Court in the case of Deutsche Grammophon Gesellschaft mbH v. Metro-SBGrossmarkte GmbH & Co[92], a matter relating to copyright infringement. A company, the appellant, was manufacturing certain records under a German copyright which were being marketed through an authorized subsidiary in France. When an independent importer, the respondent, tried to resell the products in Germany after having purchased them in France, a suit was brought against him by the appellant, alleging that its right had not been exhausted because the records not were marketed in German territory but only abroad. The Court, applying the concept of community exhaustion, opined that as long as the first authorized sale was with the consent of the holder of the intellectual property, the place of such sale would be irrelevant for the purpose of preservation of his exclusive rights. If exhaustion was to be permitted nationally, it would then permit manufacturers to get the common market portioned by restricting interstate trade which would entirely be antithetical to the aims of the European Community Treaty.

The Court sought to legally justify its decision on the basis of a conjoined reading of Articles 30 and 36 of the European Community Treaty. Broadly, as per Article 30, all quantitative restrictions on imports, subject to the caveats contained under Article 36, are prohibited.[93] An exception has been charted out by Article 36 which provides that a restriction which justifies itself on the grounds of protection of industrial property and intellectual property would be permitted provided that it would not result in any arbitrary discrimination between disguised trade restriction or competing products.[94] Perusal of the decision makes it clear that Court's conclusion was not based on an analysis of the extent of plausible extension of intellectual property rights but instead the effect of granting of such a right on the cause of integration of the common market.

iii. Considerations under the Trademark Law

Trademark holders in Europe sought protection, prior to the enactment of the Trademark Directive (TMD) 89/104, under Article 28 read with Article 30 of the Treaty of Rome that provided that no quantitative restrictions could be imposed by any state on imports except when the restrictions that protect commercial and industrial property. Reconciling and balancing the fundamental aim of having a single market with free movement of products in the Community was the essential purpose with which the Treaty was enacted in contrast to fundamental interest of protecting the commercial and industrial property rights.[95] The decisions pronounced by the European Court of Justice under the said provisions of the Treaty served as a determining factor as to whether an exercise of intellectual property rights, that prohibited or restricted any sort of trade amongst Member States, was justified if that served a purpose of safeguarding rights that

92 [1971] CMLR 631.
93 *Ibid.*
94 *Supra* note 89.
95 *Deutsche Grammophon* v. *Metro GmbH* [1971] E.C.R. 487.

constituted "essential function" or the "specific subject matter" of the intellectual property rights concerned.[96]

To understand the law of European Union on parallel imports, one would have to see to it in two categories:

(a) First Sale- outside the European Economic Area (EEA): Before TMD was enacted, it was uncertain as to whether principle of international exhaustion was advocated by Article 28 read with Article 30 of the Treaty to permit parallel imports of product placed in the market outside European Economic Area. The approach adopted by the Member States differed in practice, with some applying a rule of Community exhaustion while others applying the rule of international exhaustion.[97] However, after the introduction of Article 7, the main argument now was whether the member states were free to adopt or reject the principle of international exhaustion, as both the TMD as well as the CTMR had not made any mention. The Explanatory Memorandum for the Directive[98] discusses that the approach initially indicated clearly that the Commission's intention was adoption of international exhaustion. However, the intention was soon changed.

The Explanatory Memorandum published in 1984,[99] to the amended proposal for the CTMR mentioned that because of the absence of reciprocity in nations outside the EEA was likely to result in discrimination against the industry within the EEA; the debate was closed and it was clarified that international exhaustion was not adopted by EEA. This was backed by the interpretation adopted by ECJ of Article 7(1) in the case of Silhouette International Schmied GmbH & Co KG v. Hartlauer Handelsgesellschaft GmbH[100] wherein it was opined that the national rules which provided for exhaustion of trademark rights regarding products under a trademark put on the market by the owner of the trademark or with his consent outside the EEA were contrary to Article 7(1). However, the Commission still had hopes that international exhaustion may be introduced by bilateral or multilateral agreements, sometime in the future and that Article 7 was not absolute but qualified as exception in the form of the absence of consent of the trademark proprietor allowed him to prevent parallel imports. This exception was used by the parties advocating parallel imports in the case of Zino Davidoff v. A&G Imports[101] to argue that products that were sold with the consent of the owner in Singapore where the distributor had undertaken in a contract that he would not sell outside his specific territory as well as would impose such obligations on buyers of the said products, clearly indicated an implied consent of the trademark owner to the importation of products in the EEA. It was laid down in this case if Article 7(1) of the Directive was to be construed properly, then the consent of the owner of the trademark for the purpose of marketing the products bearing that

---

96 Report on Parallel Imports: Summary of EC Law and its Application in the EU Member States prepared by the EU Subcommittee of the Parallel Imports Committee 2004-05 *available at* http://www.inta.org/images/stories/down loads/report_eclaw.pdf (Visited on June 9, 2024).

97 *Supra* note 104.

98 COM (80) 635, Explanatory Memorandum *available at* http://aei.pitt.edu/5909/1/5909_1.pdf (Visited on July 28, 2024).

99 COM (84) *55*, Explanatory Memorandum, Explanatory Memorandum *available at* http://aei.pitt.edu/*5757*/1/*5757*.pdf (Visited on July 28, 2024).

100 [1998] ECR I-4799.

101 [2002] RPC 20.

trademark within the EEA, the products that had been previously placed by the trademark owner or with his consent on the market outside the EEA, the consent may be implied with an inference needed to be drawn from facts and circumstances that occur prior to, simultaneous with or subsequent to the placing of the products in the market outside the EEA. This is demonstrative of the fact that there has been renunciation, by the trademark owner, of his right to oppose the placement of the products on the market within the EEA.

(b) First Sale- Within the European Economic Area (EEA): Before the exhaustion principle was explicitly codified, the leading cases in the year 1970s established a series of rules regarding exhaustion of rights within the European Union. One of the most important of such rules in respect of trademarks was that once the trademark owner or someone else with his consent, place those goods in the market of a Community which are protected under a trademark, it exhausts the proprietary rights of the owner throughout the Community thereby allowing the rules of free movement to prevail.[102] The ECJ established the concept of regional exhaustion while interpreting the Treaty. As per Article 7, movement of genuine products is not restricted within the EEA. However, Article 7 is qualified and not absolute. When the products are marketed within the EEA, the rights of the trademark owner will not be exhausted in the following three instances:

(i) Consent: Parallel imports can be prohibited and a trademark owner will not exhaust his rights if sale of products is made without his consent. In the case of Sebago,[103] that happens to be leading case on this point, the ECJ opined that consent of the trademark owner for the marketing of products within EEA which are identical to the products for which exhaustion is claimed was not sufficient. It was required to be proved of there was consent of the trademark proprietor for the actual products in question. The consent has to be expressed positively and should unequivocally demonstrate that the owner of the trademark had renounced his intentions to enforce his exclusive rights.[104]

(ii) Legitimate Reasons: Though, principle of regional exhaustion has been recognized under Article 7 of TMD 89/104, however, trademark owner has been granted a right to prohibit further commercialization of products if a 'legitimate reason' exists. One of such legitimate reasons could be change or impairment in the condition of products after having been put in the market. 'Legitimate reason' may refer to 'reason specifically provided for by law'. Even if products have been marketed with the consent of trademark owner, its parallel import can still be prohibited if such products contravene with the local regulations regarding ingredients-labelling because their prohibition would be 'legitimate' as commanded by law. In the case of Colgate-Palmolive v. Markwell Finance,[105] where Colgate, manufactured in Brazil had different ingredients than the UK variant, parallel importation thereof was allowed to be prohibited. Similarly, in the case

---

[102] *Centrafarm* v. *Winthrop* [1974] ECR 1183.
[103] *Sebago Inc and Ancienne Maison Dubois et Fils SA* v. *GBUnic SA* [1999] ETMR 681.
[104] *Zino Davidoff SA. A& G Imports Ltd; Levi Strauss & Co and Levi Strauss (UK) Ltd* v. *Tesco Stores, Tesco plc and Costco Wholesale Ltd.* [2002] ETMR 109.
[105] 1988 RPC 283.

of London Borough of Backney v. Cedar Trading Ltd.[106], cans of Coca-Cola which were imported from the Netherlands and had the ingredients listed in the Dutch language, were not permitted to be sold in the UK.

(iii) Goods Changed or Impaired after having been put on the market: This is one of the reasons mentioned under Article 7 itself explicitly. In a case[107] decided under the national law of Germany, there terms 'change or impairment' were interpreted and the procedure of dying in garish colours, bleaching, as well as conversion of Levi's jeans into shorts was considered as modification that was held to be affecting the Levi's brand to such an adverse extent that defence of exhaustion was not permitted. Sometimes the parallel importer is required to relabel or rebrand the imported products with the trademark of the country in which they are imported in order to sell his such parallel imported product, especially in case where different marks are used in different countries. The question in such a case is whether such an act of rebranding/relabeling/repackaging would constitute a change or impairment thereby making it a legitimate reason for prohibiting parallel importation. However, this answer is dependent on facts of each case. Though repackaging/relabelling/rebranding would be considered essential to avoid customer confusion as to origin thereby upholding the purpose of the trademark, but the manner and form of such repackaging/relabelling/ rebranding would be the deciding factor. For instance, in a case where an adaptor, of which the origin was not clear, was included in the boxes of Sony PlayStations so that they could be connected to British television, the Court opined that it was a sufficient change to enable prohibiting the parallel importation.[108]

V. Conclusion

The question of whether parallel imports should be allowed on the theory of intellectual property exhaustion due to the first sale or commercial use of a product exploiting such rights is still up for debate. Though the common consensus is that developing countries support parallel imports while wealthy countries oppose them. Regarding the status of parallel imports in the USA, they may be allowed if the products are correctly branded in accordance with customs regulations. In the United States, the idea of material difference is adhered to, and the threshold for such differences has been kept very low in order to preclude nearly all parallel imports. Since the territoriality principle greatly dominates the trademark industry in the United States, parallel imports that damage the reputation of the trademark owner by confusing consumers about the origin of the goods are forbidden.

However, the European Union has a policy of regional exhaustion, which allows for the importation of commodities that are sold in the European Economic Area in parallel. The trademark owners may nevertheless be able to stop the legitimate parallel import of goods that

---

106 [1999] ETMR 801.
107 *Dyed Jeans Bundesgerichtshof* Case 1 ZR 10/93, [1997] ETMR 530.
108 *Sony Computer Entertainment* v. *Tesca* [2000] ETMR 102 (HC).

are offered for sale outside of the European Economic Area. Several case statutes list strict requirements that importers must adhere to in order to shield themselves from legal liability, even while importing into EEA member states. Parallel importation within the EU would likewise be forbidden in the event of valid justification. However, the specifics of the case and the mark in question would determine what would constitute a valid justification. Therefore, it is apparent that even while parallel importation is a problem on a global scale, the TRIPS agreement has left the exhaustion concern unresolved. TRIPS addresses the issue, but it also specifies that there is no resolution on the subject. As a result, each agreement member country is allowed to determine how their own national laws and courts will handle intellectual property exhaustion and parallel imports.

But what's really required is a guarantee that enacting a national law that supports parallel imports won't be viewed as an unfair trade practice in and of itself, making it illegal under the laws of the relevant individual nations or regional group.

Beyond Morphing - Unravelling Deep Fake Technology And Its Legal Analysis

CHANDRA KANT SINGH & PRIYA BANSAL

Chandra Kant Singh & Priya Bansal 2nd Year Law Students of Dr. Ram Manohar Lohiya National Law University, Lucknow

Abstract

"When reality intersects with fabrication and ethical lines begin to fade, deepfakes take hold." Artificial Intelligence has evolved extensively from life-soothing to life-distorting techniques, producing illusions that initially seem real, and eventually are the tricks of the light.This pseudo-reality, created by deepfake technology, has recently caused significant turmoil on the internet. It has targeted not only Indian actors and politicians but also celebrities from around the world. DeepFake is a technologically advanced form of digital deceit which utilizes habitual intelligence to alter visual-aid auditory contests, often leading to realistic impersonations thereby challenging traditional means of verification. Despite its benefits, like customized content for entertainment purposes, virtual avatars, etc, it also brings significant risks like creating financial scams, pornography, privacy concerns, and immeasurably more ramifications. Law is the foundation of society; an absence of it results in tyranny. The paper scrutinises India's existing legal landscape concerning deepfake technology by interpreting current laws related to privacy, cybercrime, and information technology. Furthermore, it identifies the gaps and inadequacies that hinder its effective regulation. Following this, the paper critically analyses the deep fake laws in various U.S. states, pointing out their strengths and inconsistencies. The paper recommends amending US laws to address this advanced technology adequately in light of the local demands and difficulties.

I. Introduction

The entire geopolitical world was taken aback when a video purportedly displayed Ukrainian President Volodymyr Zelenskyy urging his compatriots to surrender to the Russian army. However, to everyone's surprise, it was a fabricated video generated using machine learning technology where his voice and video clips were used to create an illusion. The technology in the picture is Deepfake, which involves machine learning, i.e., Generative Adversarial Networks (GAN). It will be a bolt from the blue if someone says today that they have never encountered a deep fake. Yes, maybe the technical terminology associated would have kept them unaware. Still, in the everyday world, in some form or another, we come across bogus and fabricated videos, images, and audio, which often go unnoticed as spurious. Such is the efficiency of tech geeks, slang for technological experts. Oxford described deepfake as: 'Any of various media, esp. a video, that has been digitally manipulated to replace one person's likeness convincingly with that of another, often used maliciously to show someone doing something that he or she did not do.' This term originated

when a Reddit moderator created a subreddit named 'deepfakes' where they posted face-swapped videos of celebrities as pornographic videos.

Synthetic media comes with a bittersweet combination as it has some significant advantages that go unnoticed by the masses. The technology can be used in the education sector where historical figures' speech or video could be recreated for better understanding or used in the field of entertainment by aiding in VFX and CGI processes to create more realistic scenes and there are even more ways to use it positively. However, it is impossible to overlook the negative aspects, from scamming, and dissemination of false news, to promoting fake pornographic content, etc. The bitterness of the technology is more prevalent, and it needs to be clamped down. The latter option could be used as a weapon of deterrence for the deep fake creators, but the same could not be promised until a thorough analysis is concluded.

In India, Deepfakes fall under the jurisdiction of the Information Act, 2000, Indian Penal Code, 1860, Digital Personal Data Protection Act, 2023, Information Technology Rules, 2021 as there is no specific legislation dealing with Deepfakes. States of the USA, Washington, Texas, and New York'sUSA- Washington, Texas, and New York laws are examined thoroughly, and favourable characteristics are highlighted that might inspire Indian lawmakers to enact better laws in the nation. Plausible solutions to the issues found in the existing laws are given to bridge the gap.

II. A National Perspective on the Legal Challenges in Implementation

Deepfake, a term that has been in the limelight lately owing to the incident with Rashmika Mandanna[9], a renowned Bollywood actress, where a video of her being involved in sexual activities went viral. The video was said to be fake, and it was generated using deep learning algorithms and Generative Adversarial Networks (GAN).[1] Possibly, this is not the first instance of the misuse of this technology, and the victims have ranged from the entertainment industry to the politics of nations by circulating morphed videos of politicians. Instances of misuse of deepfakes have substantiated the fact that the technology could be misused, if the same is not regulated soon, perhaps a catastrophe is imminent. The Union Minister for Electronics and Information Technology (MeitY), Ashwini Vaishnav has addressed the issue *'India will come up with new regulations to tackle deepfake.'*[2] and further it was said the *focus would be on 'four pillars', which include (I) detection of deep fakes, (II) prevention on spread of such content,(III) reporting of these including ramping up existing mechanism and (IV) compliance by social media platforms.*[3] It is evident from the statement of the Union Minister that the government has taken cognizance of this issue and is possibly working on the same. However, the amount of time to formalize these concepts will be normous, and due to the rapid rise[4] In

[1] Shubham Pandey and Gaurav Jadhav, 'Emerging Technologies and Law: Legal Status of Tackling Crimes Relating to Deepfakes in India' (*SCC Online Blog*, 17 March 2023) <https://www.scconline.com/blog/post/2023/03/17/emerging-technologies-and-law-legal-status-of-tacklingcrimes-relating-to-deepfakes-in-india/> accessed on 12 January 2024

[2] 'New regulations to tackle deepfakes soon: IT Minister Vaishnaw' (*The Indian Express*, 23 November 2023) < https://indianexpress.com/article/india/new-regulation-deepfakes-soon-vaishnaw-social-mediaplatforms-9039093/> accessed on 12 January 2024

[3] *Ibid*

[4] 'Sumsub Research: Global Deepfake Incidents Surge Tenfold from 2022 to 2023' (*Sumsub*, 28 November 2023) <https://sumsub.com/newsroom/sumsub-research-global-deepfake-incidents-surge-tenfold-from-2022-to-2023/> accessed on 14 January 2024

misuse of deepfakes , laws regulating the practice must be developed. There could be grave repercussions if the government does not propose new legislation or amend current legislation that could to some extent prosecute as well as create a state of deterrence amongst the perpetrators.

Although there isn't a specific law in India that addresses deepfake in the present scenario, there are pre-existing laws that may partially address the issue. A few laws that indirectly deal with deepfake are the Information Technology Act,2000[5]; the Indian Penal Code[6], 1860; and the Digital Personal Data Protection Act, 2023[7].

Multiple questions might arise in the minds of lawmakers and citizens regarding , which are:

- Are the present laws capable of dealing with deepfakes?
- If not, is there a need for separate legislation or amendment in the present laws will suffice?

To answer these questions the research paper deals with the thorough analysis of the existing laws.

III. Information Technology Act, 2000: A Thorough Analysis

In many facets of life, the adage "old is gold" is accurate; but, due to evolving circumstances and recent developments in the technological field, the authors are unable to make the same assurances on the laws. Only a few must have predicted in 2000 that, twenty years later, technology would emerge, changing our perception of reality. This frightening development needs immediate remedy, and one law that might address the problem of deepfake is the Information Technology Act, 2000.

Nexus between Section 66D[8] and Section 66C[9]

Section 66D: states *'Punishment for cheating by personation by using computer resource Whoever, by means of any communication device or computer resource, cheats by personation, shall be punished with imprisonment of either description for a term which may extend to three years and shall also be liable to fine which may extend to one lakh rupees,'* The perplexity is to establish a link between personation and deepfake. To begin with, the definition of personation is – *'to act or play the part of'*[10] Understanding the definition

[5] Information Technology Act 2000
[6] Indian Penal Code 1860
[7] Digital Personal Data Protection Act 2023
[8] Information Technology Act 2000, s 66D.
[9] Information Technology Act 2000, s 66C.
[10] 'Personate' (*Collins*) <https://www.collinsdictionary.com/dictionary/english/personate> accessed on 16 January 2024

of deepfake in detail will help one establish the association. Deepfake[11] is defined as using technology to create the appearance that a real person has done or said something, when in fact it was not done at all, and this is what personation means. To make this appear real, the identity of the targeted person is stolen. This implies that there is an identity theft of that person and the same is covered under **Section 66C**, which reads as *'Punishment for identity theft.–Whoever, fraudulently or dishonestly make use of the electronic signature, password or any other unique identification feature of any other person, shall be punished with imprisonment of either description for a term which may extend to three years and shall also be liable to fine which may extend to rupees one lakh.'* The video in which the American President, Joe Biden[12] was seen making transphobic remarks could be one example of identity stealing. At first, it may seem that the provision is a way to penalise illegal deepfake creators, but there is a major flaw in it. The flaw is that there is no mention of the machine learning algorithms that deepfake uses to generate its results, which could provide an opportunity for the offenders to escape.

Section 66E[13]

Referring to the previously given example of Rashmika Mandanna[14], another sub-section of this provision came into the picture when the Delhi Police filed the case in a matter under Section 66E.

Section 66E reads as: *'Punishment for violation of privacy.–Whoever, intentionally or knowingly captures, publishes or transmits the image of a private area of any person without his or her consent, under circumstances violating the privacy of that person, shall be punished with imprisonment which may extend to three years or with fine not exceeding two lakh rupees, or with both.'* Applying the provision in the instance of deepfake is complicated.

The actual distinction is made by the sentence that reads, "publishes or transmits the image of a private area of any person without his or her consent." It states that publishing or transmitting an image of that person's private parts is illegal, but in deepfake pornography cases, the person targeted is not the one whose private parts are exposed—rather, it is someone else's. This defeats the argument that the targeted person's right to privacy is being violated by disclosing their private parts instead the private parts of the person whose face is superimposed in the video are exposed.

Section 67[15]

[11] 'Deepfake' (*Merriam-Webster*) < https://www.merriam-webster.com/dictionary/deepfake> accessed on 16 January 2024
[12] Jake Horton & Shayan Sardarizadeh, 'False claims of 'deepfake' President Biden go viral' (*BBC*, 28 July 2022) <https://www.bbc.com/news/62338593> accessed on 16 January 2024
[13] Information Technology Act 2000, s 66E.
[14] *Id* at 3
[15] Information Technology Act 2000, s 67

Women have been the primary target of deepfakes in the form of revenge as 96 percent of deepfake cases fall under the above-mentioned category.[16] Following the publication of lewd films and images of female influencers, such as Alia Bhatt[17] and Katrina Kaif[18], one may wonder if any existing Indian laws could protect them from publishing such lascivious content.
Section 67 may provide some insight regarding the same.

However, since it doesn't explicitly mention deepfakes, people might be unable to associate with it. The creators of revenge porn will be covered in this provision as in the line '*if its effect is such as to tend to deprave and corrupt persons who are likely, having regard to all relevant circumstances, to read, see or hear the matter contained or embodied in it*'. When someone uses deepfake to create revenge porn, their face is superimposed on the body of the person engaging in sexual activity. This gives the illusion that the targeted person is engaging in the activity, which damages the reputation due to the difficulty of concluding if the information is real or fake. Sections 67A[19] and 67B[20] will apply to the victim who is a major and a minor, respectively.

Section 72[21]

The definition of privacy has always been subjective and contentious. According to Cambridge University[22], privacy is defined as "the state of being alone." This suggests that the essence of privacy is the ability to be left alone. However, deepfakes have seriously shaken this concept by controlling people's privacy by sharing any image, video, or audio without permission, infringing on their fundamental right to privacy.

As stated in the above-mentioned statement, Section 72 may address this issue.: *"**Penalty for Breach of confidentiality and privacy.**– Save as otherwise provided in this Act or any other law for the time being in force, if any person who, in pursuance of any of the powers conferred under this Act, rules or regulations made thereunder, has secured access to any electronic record, book, register, correspondence, information, document or other material without the consent of the person concerned discloses such electronic record, book, register, correspondence, information, document or other material to any other person shall be punished with imprisonment for a term which may extend to two years, or with fine which may extend to one lakh rupees, or with both.'*

[16] Sally Adee, 'World's First Deepfake Audit Counts Videos and Tools on the Open Web' (*IEEE Spectrum*, 7 October 2019) <https://spectrum.ieee.org/the-worlds-first-audit-of-deepfake-videos-and-tools-on-the-open-web> accessed on 18 January 2024
[17] Bijin Jose, 'Alia Bhatt is the latest to fall prey to deepfakes: 12 ways to stay safe online' (*The Indian Express*, 30 November 2023) <https://indianexpress.com/article/technology/artificial-intelligence/alia-bhattdeepfake-video-ways-to-stay-safe-online-9045902/> accessed on 18 January 2024
[18] 'Katrina Kaif is latest victim of deepfake tech after Rashmika Mandanna, fake pic of diva from 'Tiger 3' goes viral' (*The Economic Times*, 10 November 2023) <https://economictimes.indiatimes.com/magazines/panache/now-katrina-kaif-is-latest-victim-of-deepfake-techtowel-clad-pic-from-tiger-3-goes-viral/articleshow/105040415.cms?from=mdr> accessed on 18 January 2024
[19] Information Technology Act 2000, s 67A.
[20] Information Technology Act 2000, s 67B.
[21] Information Technology Act 2000, s 72.
[22] 'Privacy' (*Cambridge Dictionary*) <https://dictionary.cambridge.org/dictionary/english/privacy#google_vignette> accessed on 18 January 2024

The gaps in this provision are listed:

- **Absence of contemporary sources:** The main sources that the makers of deepfakes use are images, videos, and audio files. These are not mentioned at all. While it is possible to cover these sources if we read between the lines of the clause, it is best to state clearly which sources might be misused.

- **Inadequate Punishment:** Another problem with this clause is that the maximum sentence of two years is not adequate. Because of the invasion of privacy and the unfathomable effects it could have on the victim, this is a major offence with dire consequences.

IV. Digital Personal Data Protection Act, 2023

Social media platforms have been the chief source for the dissemination of deepfakes since they have become a convenient way for offenders to reach a large audience, notably when the topic is contentious or involves a well-known personality. This implies an urgent need to regulate social media platforms to curb the spreading of the matter as soon as possible. Digital Personal Data Protection Act (DPDP), 2023 is one recent law that may partially cover the issue of Deepfake as it is concerned with the protection of individuals' personal data from misuse by Data Fiduciaries or social media platforms.[23]

Applicability of the DPDP Act

Sections 3(a)[24] and 3(b)[25] of the Act will be applicable if the processing is carried out in both India and outside respectively, but ambiguity could be traced in section 3(c) which deals with the non-applicability of this act.

Section 3(c)(i)[26]- This clause states that: *'not apply to— (i) personal data processed by an individual for any personal or domestic purpose'*. This poses the question of what is meant by *'personal or domestic purpose'*.

Additionally, a crucial question about deepfake could be raised: How will the common populace be protected in case of a breach of personal data if there is ambiguity in the definitions of *personal or*

[23] Sarvagya Chitranshi, 'The "Deepfake" Conundrum - Can the Digital Personal Data Protection Act, 2023 Deal with Misuse of Generative AI?' (*Indian Journal of Law and Technology*, 23 December 2023) <https://www.ijlt.in/post/the-deepfake-conundrum-can-the-digital-personal-data-protection-act-2023-deal-withmisuse-of-ge> accessed on 20 January 2024
[24] Digital Personal Data Protection Act 2023, s 3(a)
[25] Digital Personal Data Protection Act 2023, s 3(b)
[26] Digital Personal Data Protection Act 2023, s 3(c)(i)

domestic purpose under this act? The act promised, in the beginning, the protection of individuals' data and its lawful usage by way of processing the data.

Section 3(c)(ii)[27]- This brings another question of doubt regarding the applicability of the act.

It states: '*not apply to—*

(ii) personal data that is made or caused to be made publicly available by—

(A) the Data Principal to whom such personal data relates.'

Therefore, the data that has been publicly made available by the *Data Principal* would not be covered under the ambit of this clause. Here, Data Principal[28] 'means the individual to whom the personal data relates'. One of the most significant problems concerning the act is that Data principals will not be protected if they publicly make the data available and this defeats the purpose of the legislation. Most affected by this clause would be prominent personalities from various fields such as entertainment, politics, sports, etc. who publicly upload their data.

V. Indian Penal Code,1860

The Bharatiya Nyaya Sanhita serves as the foundational legal framework governing criminal offences in India. Its various provisions indirectly involve the concerns raised by the sophisticated form of deception. In this context, BNS's provisions related to defamation, obscenity, cheating by personation, and forgery become crucial in navigating the legal structure surrounding deepfake. The discussion will delve into specific sections of BNS, shedding light on the legal intricacies and ensuring the legal system works in tandem with the evolving technology.

Section 152[29] and Section 356[30]

Section 152 criminalises acts that express hatred or contempt towards the government established by law, whereas Section 356 deals with defamation, aiming to protect individuals' reputations from harm. Section 152 says, "*Whoever by words, either spoken or written, or by signs, or by visible representation, or otherwise, brings or attempts to bring into hatred or contempt, or excites or attempts to excite disaffection towards, the Government established by law in India, shall be punished with imprisonment for life, to which*

[27] Digital Personal Data Protection Act 2023, s 3(c)(ii)
[28] Digital Personal Data Protection Act 2023, s 2(j)
[29] Bharatiya Nyaya Sanhita 2024, s 152
[30] Bharatiya Nyaya Sanhita 2024, s 356

fine may be added, or with imprisonment which may extend to three years, to which fine may be added, or with fine."

Section 152 reads, "*Whoever, by words either spoken or intended to be read, or by signs or by visible representations, makes or publishes any imputation concerning any person intending to harm, or knowing or having reason to believe that such imputation will harm, the reputation of such person, is said, except in the cases hereinafter excepted, to defame that person*."

However, there are challenges to attract sedition and defamation as a penalised provision for deep fakes:

- Ambiguity in definition- The inherent ambiguity in the definition of sedition has already raised concerns, and incorporating yet another aspect dealing with deepfake into it without explicitly mentioning it may lead to controversies and differing interpretations. Section 356 prevents individual-centric defamation; deepfake offences may target groups and organisations or contribute to broader societal discord. Thus, the provision may fall short.

- Communication Modalities- The sections primarily focus on written or spoken communication, making it less suitable for addressing offences involving manipulated content characteristics of deep fakes. In other words, the provisions' language will not suffice the diverse forms of communication associated with synthetic media.

- Proving Malicious Intent- The criminal law is often expressed by the Latin phrase, "*actus non facit reum nisi mens sit rea*", loosely translating into an act that does not make a man guilty of a crime unless his mind is also guilty. It is challenging to prove the creator's intent as sometimes the deepfake could be created in satire or fun without the intent to harm someone's reputation. For instance, the increasing trend on social media to add songs in the form of memes (an amusing or interesting item such as a captioned picture or video or genre of items that is spread widely online especially through social media)[31] as if sung by the Prime Minister, Mr Narendra Modi.

A similar reasoning is to attract Sections 501[32] and 356[33], which regard printing and sale of defamatory matters as unlawful, which is difficult to establish as the provisions contain the words "*known to be defamatory*." The term 'matter' in the sections traditionally does not involve manipulated or created content; this can again lead to debate due to the conventional understanding of matter and not having an absolute mention of deepfake. In short, the courts may

[31] 'Meme' (*Merriam-Webster*) <https://www.merriam-webster.com/dictionary/meme> accessed on 21 January 2024
[32] Bharatiya Nyaya Sanhita 2024, s 501
[33] Bharatiya Nyaya Sanhita 2024, s 502

face difficulties applying these sections to offences involving deep fake content, as the sections have not considered the ambit of digital manipulation.

Section 292[34]

The section constitutes the legal framework that addresses offences related to obscenity in India. The section reads as follows, "*A book, pamphlet, paper, writing, drawing, painting representation, figure or any other object shall be deemed to be obscene if it is lascivious or appeals to the prurient interest or if its effect or where it comprises two or more distinct items, the effect of any of its items, is, if taken as a whole, such as to tend to deprave and corrupt persons who are likely, having regard to all relevant circumstances, to read, see or hear the matter contained or embodied in it.*"

The provision encompasses a broad spectrum of materials, encompassing various forms of expressions, and the essence of obscenity, according to the section, lies in lascivious content, appeals to prurient interests, or has an overall effect that tends to deprave and corrupt individuals who are likely to encounter it. The words are subjective in themselves and do not explicitly define what constitutes obscenity, and do not outline the criteria for determining whether particular materials are deemed obscene.

Notably, the provision indirectly includes the concept of fake and created content when it says, "*comprises of two or more distinct items*"; however, despite the seemingly comprehensive nature of the section, its applicability is confined to physical and tangible items. The limitation arises from the wording of the section, which refers to "*any other object.*" This phrasing, while broad, does not explicitly extend to encompass digital or virtual content, which has become increasingly prevalent in the modern era.

As a result, the effectiveness of Section 292 in addressing offences related to fake and created content, especially in digital form, is constrained. The legal consequences for such content being treated as obscene under the IPC are not fully realised due to the legislative gap concerning the inclusion of digital content within the ambit.

Section 79[35]

The provision reads, "*Whoever, intending to insult the modesty of any woman, utters any words, makes any sound or gesture, or exhibits any object, intending that such word or sound shall be heard, or that such gesture*

[34]Bharatiya Nyaya Sanhita 2024, s 292
[35] Bharatiya Nyaya Sanhita 2024, s 79

or object shall be seen, by such woman, or intrudes upon the privacy of such woman, shall be punished with simple imprisonment for a term which may extend to three years, and also with fine."

There is a recognised gap in these laws when it comes to addressing sexual harassment through electronic means, such as deepfake crimes. Deepfake involves using technology to create realistic-looking but fabricated content, often for malicious purposes, and can include creating explicit and non-consensual material. In the context of the existing law, the absence of specific provisions addressing electronic modes of harassment, like deep fake crimes, is a significant limitation. The law was formulated in an era when electronic communication methods were less prevalent today. As a result, the law does not adequately cover the nuances and challenges of modern technology, making it essential to revisit and update legal frameworks to address emerging forms of harassment.

The initiative taken by Chattisgarh to insert clause 509B[36], which specifically addresses sexual harassment by electronic means, is commendable. The state amendment recognises the evolving nature of crimes in the digital era and aims to provide legal protection to individuals who may be targeted through online platforms. For adequate and uniform protection against online sexual harassment, it is crucial for other states and, ideally, the national legislature to consider similar amendments to their legal frameworks. This would ensure that individuals nationwide have consistent legal recourse against offences committed through electronic modes.

VI. The Legal Landscape of the United States for Deepfakes

India isn't the only nation grappling to regulate deepfakes; instead, multiple nations have stepped up to mitigate the problem promptly because of the damage deepfakes are doing to countries. The United States of America was one of the first nations where regulation of deepfakes began by enactment of the National Defense Authorization Act for Fiscal Year 2020.[37] Further, states like New York, California, Washington, Texas, Georgia, etc. also participated in regulating deepfakes by enacting their own laws. These laws must be scrutinised to check whether they are geared up or if some issues need to be fixed. Furthermore, inspiration could be drawn from these laws by Indian lawmakers to close the gaps mentioned in the research paper.

Washington's Deepfake Law

[36] Bharatiya Nyaya Sanhita 2024, s 79B

[37] Jason C. Chipman and Stephon W. Preston, 'First Federal Legislation on Deepfakes Signed Into Law' (*WilmerHale*, 23 December 2019) <https://www.wilmerhale.com/insights/client-alerts/20191223-first-federallegislation-on-deepfakes-signed-into-law> accessed on 23 January 2024

The Senate of Washington passed a law on April 6th, 2023 relating to defining synthetic media in campaigns for elective office and providing relief for candidates and campaigns. The primary object of the act is to shield a candidate from any kind of synthetic media usage that might be against the said candidate and provide reasonable damage caused due to the act. The abstract spirit behind the law is to strengthen democratic elections by curbing any kind of illegal usage of artificial intelligence (AI) which might hamper the smooth process of voting.

Accuracy of the Definition

Synthetic Media[38]: The definition of synthetic media has been beautifully drafted as covers all the aspects that might be misused such as image, video, or audio through AI. Further, it has mentioned the mechanism that is used to create deepfakes i.e. Generative Adversarial Network (GAN). It reads as: *'an image, an audio recording, or a video recording of an individual's appearance, et speech, or conduct that has been intentionally manipulated with the use of generative adversarial network techniques or other digital technology'*. Later, Section 2(1)(a)[39]and Section 2(1)(b)[40] state the ways through which deepfakes might be used i.e. to deceive or create a fundamentally different impression of action, appearance, etc. Section 2(1)(a) and Section 2(1)(b) read as:

(a) A depiction that to a reasonable individual is of a real individual in appearance, action, or speech that did not actually occur in reality; and

(b) A fundamentally different understanding or impression of the appearance, action, or speech than a reasonable person would have from the unaltered, original version of the image, audio recording, or video recording.

At this junction, the above-mentioned definition of synthetic media or fabricated media could be called as perfect as it covers almost all the domains of deepfakes. Inspiration could be taken from this definition by Indian lawmakers while amending previous legislation or drafting a new law regarding deepfakes. Inserting a definition like the above-mentioned would be able to encapsulate the data or media that is produced by deepfakes which could be penalised if illegal.

Relief to the victim: Remedy of injunction is provided under Section 2(2), which reads as: '*seek injunctive or other equitable relief prohibiting the publication of such synthetic media'*. The remedy for damages is covered under Section 2(3).

[38] 42, R.C.W. § 2(1) (2023).
[39] 42, R.C.W. § 2(1)(a) (2023).
[40] 42, R.C.W. § 2(1)(a) (2023).

The remedies provided under the above-mentioned provisions are civil, which prima facie appears to be adequate. But this might not be apt because of the danger and damage, this technology's usage might cause to the whole nation or world. 2024 is a crucial year in the political world due to the major elections to be held across nations from India, the USA, Indonesia, Russia, and many more.[41] After the entry of deepfakes into the political realm, it is very important to put penal measures to create deterrence in the minds of illegal deepfake creators. The addition of criminal punishment could be one way to solve this problem.

a) Texas

Chapter 21 of the Penal Code of Texas has been amended by adding Section 21.165[42] to read as follows- '*Unlawful Production Or Distribution Of Certain Sexually Explicit Videos.*' The act came into effect on September 1, 2023. The act defines deepfake video as '*a video, created with the intent to deceive, that appears to depict a real person performing an action that did not occur in reality.*'

The elements of the crime include-

- The person produces or distributes a deepfake.
- It depicts the person with exposed intimate parts or engaged in sexual conduct.
- The action is done without the effective consent of the person.

While this amendment is a step towards addressing the issues related to deepfake videos, it is crucial to take note of its limitation which is its limited scope-The amendment explicitly targets deepfake videos and does not extend its ambit to cover other forms of deepfake like photographs and audio recordings. The current law will not address the misleading and falsified photographs and synthetic voices, potentially misleading to false representation and deception.

b) New York

Kathy Hochul, the Governor of New York, signed Senate Bill 1042A[43] on September 29, 2023.[44] The Act is about the unlawful dissemination or publication of intimate images created by digitisation and of sexually explicit depictions of an individual. The legislation intends to protect individuals from maliciously distributing private and explicit content without their consent.

Section 1 of 245.15 of the penal law includes the elements as:

---

[41] Koh Ewe, 'The Ultimate Election Year: All the Elections Around the World in 2024' (*Time*, 28 December 2023) < https://time.com/6550920/world-elections-2024/> accessed on 25 January 2024
[42] Texas Penal Code, § 21, cl. 165 (2023).
[43] New York Penal Law, §245.15.
[44] Zach Williams, 'New York bans deepfake revenge porn distribution as AI use grows' (*Bloomberg Law*, 2 October 2023) <https://news.bloomberglaw.com/in-house-counsel/n-y-outlaws-unlawful-publication-ofdeepfake-revenge-porn> accessed on 26 January 2024

- The person must have the intent to cause harm to another individual, The individual must disseminate the still or video image.
- The person must be reasonably identifiable from the image or information displayed in connection.

The issue left uncovered is the limitation of content to images and video images, which implies leaving out other forms of explicit content, such as audio recordings, synthetic writings, or the limitation of content to images and video images, which implies leaving out other forms of explicit content such as audio recordings and synthetic writings, or any representations representations.

Section 2 explains digitization as '*to alter an image in a realistic manner utilizing an image or images of a person, other than the person depicted, or computer generated images.'* The definition is wide in its ambit as it incapsulates all computer-generated images, an amendment to not to make it restricted to imagesbut videos, and other forms of media will bridge the potential gaps in protection. The language expansion would enhance the law's relevance and effectiveness in addressing a wider range of digital manipulations. Although the provisions are not flawless, inspiration should be drawn from them to introduce laws against deepfakes in India.

VII. Solution For The Deep Fake Conundrum

The rise of deepfake technology has ushered in a new era of digital deception, posing significant threats to privacy and information security. As technology becomes more sophisticated, addressing this challenge requires a multifaceted approach, which includes legal, technological and societal dimensions.

1. *Awareness Amongst Masses*[45]-

   Public awareness is a critical component in the fight against the manipulation of media content. The rising threat of deepfake technology necessitates efforts to raise public awareness and equip individuals with the knowledge needed to navigate the digital landscape. The following ways could help generate awareness.

   - Educating the general population about the existence, capabilities, and potential dangers of deepfake technology is essential. Many individuals become susceptible to misinformation and manipulation due to a lack of awareness.
   - Governments, Non-Governmental Organisations, and technological companies should collaborate to implement widespread awareness campaigns. Each sector

[45] Mika Wesrerlund, 'The Emergence of Deepfake Technology: A Review' (2019) 9 T. I. M. REV. 39, 45

brings unique strengths, and collaboration would ensure comprehensive dissemination of information; as in this case, the Government can provide framework and support, NGOs can leverage networks, and companies can provide their platforms to reach vast audiences.

- The central aspect of spreading awareness is empowering individuals to evaluate the authenticity of media content critically and fostering a mindset that does not accept everything at face value, creating a collective defence against deepfakes.

2. *Amendments in present laws to give inclusivity to deepfakes*[46]-

Incorporating specific language that explicitly identifies deepfake-related offences and recognising the distinctive nature of these crimes would ensure a robust legal response to deepfakes.

- To enhance legal clarity and precision, amendments should incorporate terms like 'deepfake' into the definitions section of relevant laws. This will ensure that the language of the legislation reflects the technology it seeks to regulate and will establish a clear framework for judicial interpretation.
- The lawmakers should work closely in collaboration with technology experts to understand the technical intricacies of deepfake creation and detection.
- Preventive measures like stringent licensing requirements for deepfake creation tools should be incorporated to minimise the occurrence and opportunity for everyone to indulge in malicious activities.
- Engaging with international counterparts, sharing best practices and knowledge to collectively prosecute against cross-border deepfake offences due to the global nature of the internet and digital content sharing.

3. *Stricter Punishments*-

To effectively counter the malicious use of deepfakes, it is imperative to establish a legal framework that not only identifies and defines offences related to deepfakes but also imposes stricter punishments on those engaged in the activities. This framework will punish the wrongdoers for their actions and deter potential offenders from participating in the illegal act.

- The offenders should face substantial fines and imprisonment as punishment. The severity of these legal consequences should be proportionate to the potential harm caused by deepfake.
- Legal frameworks should be subjected to periodic review as the technology evolves, and so should the legal responses. Lawmakers should proactively identify the

[46] Jack Langa, 'Deepfakes, Real Consequences: Crafting Legislation to Combat Threats Posed by Deepfake' (2021) 101 B.U.L. REV. 761, 797

challenges and assess the effectiveness of existing laws to make necessary adjustments.

4. Investments in Research and Development[47]-

A strategic initiative for staying ahead of the curve is crucial, ensuring the country is well-equipped to detect deepfakes effectively. It calls for governments, private companies, and academic institutions to make substantive investments in research and development.

- Machine learning stands at the forefront against deepfakes. Investments should be directed towards advancing machine learning algorithms.
- Research in forensic analysis tools should also be prioritised to establish reliable methods for tracing the source of false content.
- Public-private partnerships will create a synergy, accelerating the development of detection.
- An integrated approach ensuring a comprehensive coverage of different mediums like audio, video or photograph should be adopted.

In conclusion, by implementing the comprehensive strategy, society and law can build a resilient defence against the growing threat of deepfakes. Acknowledging the vulnerabilities of individuals, investing in research and development, enhancing legal framework, fostering collaborative efforts, and creating awareness can create safeguards in the digital age. Through these proactive measures, one can mitigate the risks posed by deep fakes and ensure a secure digital environment.

VIII. Way Forward

The detrimental power to damage one's reputation or shake the whole democracy of a nation is imminent if left untouched. Deepfake technology has ushered in a new era of challenges and opportunities. In the time when Urfi Javed and Ranveer Singh were not only brutally trolled but were also facing criminal charges, even when they posted their real pictures online. When the issue changes to creating pictures, videos, or audio, why will the situation not turn chaotic? The deceptive nature of the technology cannot be ignored as it poses privacy threats, and vigilance is crucial to detect and counteract the damaging effect of deep fakes. As explored in the research paper, existing laws in India are not specifically tailored to address deepfakes. Drawing insights from the American jurisdiction, the paper provides a roadmap for Indian lawmakers to consider when crafting comprehensive legislation. As we navigate this complex terrain, a proactive approach is imperative to safeguard the integrity of information and uphold the trust of interconnected world allies.

[47] Danielle K. Citron & Robert Chesney, 'Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security' [2005] 107 CAL. L. REV. 1753.

AI Judicature: Navigating the Future of Justice

NIKHIL BAJPAI

Abstract

AI technology is becoming more and more significant in numerous facets of everyday life. Thus, the manner in which people operate is one of the numerous aspects of our daily situations that AI is changing. According to projections, many facets of human activity will either be replaced or supplemented by more recent technology. Furthermore, the development of sophisticated machinery is altering both the legal profession and the way judges render judgments in court proceedings. The purpose of this paper is to investigate the ways in which artificial intelligence is impacting judicial systems and the problems associated with its use in legal proceedings, especially in the context of law enforcement.

I. Introduction

Since the invention of machines, many have been captivated by the idea of building intelligent machines[1]. The conventional methods of creating artificial intelligence have produced flawless outcomes ever since engineers began to understand that computers could be utilized for purposes other than numerical computation. Artificial intelligence is present in a number of computers nowadays, and researchers have been attempting to replicate human intellectual behavior in computer programs.

Artificial intelligence holds great promise for bettering our lives[2]. In fact, in some cases, AI-based systems are now more accurate at identifying ailments than medical professionals. AI has also made it possible for organizations to do more with less money, which has positive effects on the access and affordability of services of all kinds.

Though there isn't a single, widely accepted definition, most explanations of AI have the following four features:

i) structure-wide that thinks like people,

ii) the structure that acts like humans,

iii) structure that thinks logically,

[1]J.N. Kok, P. Van Der Putten, "Artificial Intelligence: Definition, Trends, Methods, and Cases" Knowledge for sustainable development: an insight into the Encyclopedia of life support systems, 1, p. 1095-1107, (2002).
[2]V. KRISHNAMURTHY, C. BAVITZ, L. KIM, "Artificial intelligence and Human rights", 1, September 25, 2018.

iv) structure that acts rationally.

Though AI can be programmed in a variety of ways, machine learning as well as deep neural networks are the two primary programming types. The first approach relies on an electronic initiative's ability to accept fresh data without human involvement. "The method through which an electronic device has the ability to enhance its own capabilities by constantly integrating information into a preexisting statistics framework"[3] is the precise definition of artificial intelligence. Specifically, the computer gets a certain quantity of data, and then it uses that data to adjust the algorithms.

The second type is an aspect of computer technology that mimics how a human brain processes information and forms trends to aid in making choices. Specifically, deep learning, which is commonly referred to as a "deep neural learning" or "deep neural network," is "... an area of artificial intelligence in AI that has networks competent of acquiring knowledge uncontrolled from information that is unorganized or unlabeled"[4]. Furthermore, there are two "buckets" into which the vast array of technologies and methods that fall under the "Artificial Intelligence umbrella" can be divided[5]. The first, which can be summed up as "knowledge-driven systems," is related to the idea of producing actions through inference from a set of axioms[6]. These systems are adept at making optional decisions within a particular domain according to established rules, but they are unable to automatically learn from or apply the data they have accumulated over the years. The second category is a collection of tools that "enhance their ability to make decisions consistently through statistics learning." The tremendous drop in storage costs, the exponential increase in computer processing capacity, and the consequent speed of gathering data have all contributed to the development of this new wave of technology. This group of technologies encompasses self-driving automobiles, technology that recognizes faces for law enforcement, and methods for processing natural language for automated material regulation and translation[7].

However, modern technology can be implemented to enhance the communication and information-gathering services provided by the judiciary, aid in the execution of laws pertaining to minor claims processes, and promote international collaboration amongst judicial agencies. In terms of fostering clarity and supporting uniformity in legal precedent, this may be helpful. In addition, according to Thomas Julius Buocz, "AI can be utilized as an instrument for evaluating rulings from courts, having the aim of helping judges make decisions on particular legal concerns by helping identify standards related to cases"[8].

Lastly, it should not be understated that there may be risks associated with the judicial decision-making process in structured computer databases and that suitable precautions must be taken. In actuality, there may be issues with security, privacy, and the safeguarding of personal information. In this way, it is crucial to

[3]https://www.merriam-webster.com/dictionary/machine%20learning last visited on 01/05/2024
[4]https://www.investopidia.com/terms/m/deep-learning.asp last visited on 01/05/2024
[5] Raso, Filippo, Hannah Hilligoss, Vivek Krishnamurthy, Christopher Bavitz, and Kim Levin, "Artificial Intelligence & Human Rights: Opportunities & Risks" Berkman Klein Center for Internet & Society Research Publication, 2018 accessed at https://dash.harvard.edu/bitstream/handle/1/38021439/2018-09_AIHumanRights.pdf?sequence=1&isAllowed=y
[6] Bibel, Wolfgang, "Artificial Intelligence in a historical perspective" AI Communications. 27(1). At pg 87-102, (2014) accessed at https://www.researchgate.net/publication/262159847_Artificial_Intelligence_in_a_historical_perspective
[7] Supra *id 5*
[8] Ibid.

ensure that an individual's right to an impartial jury along with other fundamental principles is respected while using AI in court.

II. Definition and Scope of AI in Legal Context

Artificial intelligence (AI) in the legal context refers to the application of computational algorithms and machine learning techniques to assist in various aspects of legal practice and decision-making. It encompasses a broad range of technologies designed to automate tasks, analyze data, and provide insights relevant to legal matters. AI in the judicial system encompasses both software applications and hardware systems that aid legal professionals in legal research, case management, document review, predictive analytics, and other functions.

A. The scope of AI in the legal context includes:

AI-powered tools can sift through vast volumes of legal documents, statutes, case law, and academic literature to identify relevant precedents, statutes, and arguments. Natural language processing (NLP) algorithms enable these tools to understand and analyze complex legal texts.

AI algorithms can automate the process of reviewing and analyzing documents for relevance, privilege, and responsiveness in litigation. This includes tasks such as e-discovery, contract analysis, and due diligence in mergers and acquisitions.

AI systems can analyze historical case data to predict case outcomes, assess litigation risk, and provide recommendations for legal strategy[9]. These predictive models rely on machine learning algorithms trained on large datasets of past legal cases.

AI-powered virtual assistants and Chatbots can provide legal guidance, answer legal questions, and assist with routine legal tasks[10]. These tools leverage natural language understanding and dialogue management techniques to interact with users in conversational interfaces.

B. Historical Evolution of AI in Law:

The use of AI in law dates back several decades, with early efforts focused on automating routine legal tasks and developing expert systems for legal reasoning. Some key milestones in the historical evolution of AI in law include:

1960s-1970s: Early research in AI and law focused on building rule-based expert systems to model legal reasoning in specific domains, such as tax law and contract law. Systems like MYCIN and DENDRAL demonstrated the potential of AI to emulate human expertise in decision-making tasks.

[9] Solove, D. J., & Hartzog, W. "The Cambridge Handbook of Consumer Privacy" Cambridge University Press, 1st Edition, 2018
[10] Citron, D. K., & Pasquale, F. "The scored society: due process for automated predictions" Washington Law Review, 89(1), at pg. 1-32, 2014.

1980s-1990s: The development of case-based reasoning (CBR) systems and legal expert systems continued to advance, with applications in legal drafting, case analysis, and legal education. Notable projects during this period include the EUROPA project and the Legal Knowledge Interchange Format (LKIF).

2000s-2010s: The proliferation of digital technologies and the internet led to the emergence of AI-powered legal research platforms, such as Westlaw and LexisNexis. Advanced machine learning techniques, including deep learning and natural language processing, enabled more sophisticated applications of AI in law, such as predictive analytics and document review.

C. Current Landscape of AI Integration in Judicial Processes:

In the contemporary legal landscape, AI technologies are increasingly integrated into various judicial processes to improve efficiency, accuracy, and access to justice. Some examples of AI integration in the judicial system include:

AI-powered legal research platforms, such as ROSS Intelligence and Casetext, leverage machine learning algorithms to provide comprehensive search capabilities and relevant case law summaries[11].AI-driven e-discovery platforms, such as Relativity and Disco, use advanced analytics and machine learning to streamline the review process, reduce costs, and identify relevant documents more efficiently[12].Law firms and legal departments use predictive analytics tools, such as Premonition and Lex Machina, to forecast case outcomes, assess litigation risk, and make data-driven decisions about legal strategy.AI-powered virtual assistants and Chatbots, such as DoNotPay and Legal Robot, provide legal guidance, automate routine tasks, and assist individuals with legal issues related to contracts, landlord-tenant disputes, and traffic tickets.

However, challenges related to bias, transparency, and ethical concerns must be addressed to ensure the responsible and equitable use of AI in the legal context.

III. Applications of AI in Legal Proceedings

A. Legal Research and Case Analysis

AI technologies have transformed legal research and case analysis by automating the process of sifting through vast volumes of legal documents, statutes, and case law to identify relevant information. Some key applications include:

Natural Language Processing Algorithms enable AI-powered legal research platforms to understand and analyze complex legal texts, facilitating more accurate and efficient search results[13].AI platforms leverage

[11]Law, Technology and Society: Reimagining the Regulatory Environment" by Roger Brownsword
[12] "Artificial Intelligence and Legal Decision-Making: The Wide Range of Applications and Ethical Implications" edited by JeroenKeppens, Bram Delvaux, and Frederic Petitjean
[13]he Future of the Professions: How Technology Will Transform the Work of Human Experts" by Richard Susskind and Daniel Susskind

semantic search techniques to identify relationships and connections between legal concepts, enabling users to uncover relevant precedents and arguments more effectively[14].AI tools can automatically generate summaries of legal cases, statutes, and regulations, providing users with concise overviews of complex legal issues.AI-driven legal research platforms offer analytics features that enable users to identify trends, patterns, and outliers within legal datasets, helping lawyers and researchers gain insights into legal developments and strategies[15].

B. Predictive Analytics and Risk Assessment

AI-powered predictive analytics tools analyze historical case data to predict case outcomes, assess litigation risk, and inform legal strategy. These tools leverage machine learning algorithms to identify patterns and correlations in legal datasets, enabling users to make data-driven decisions. Key applications include:

Predictive analytics models can forecast the likely outcome of legal cases based on factors such as case law, judge, jurisdiction, and parties involved.AI tools assess the likelihood of success and potential risks associated with pursuing or defending legal claims, helping lawyers and clients make informed decisions about litigation strategy. Predictive analytics models can optimize resource allocation by identifying cases with the highest likelihood of success or the greatest potential impact, enabling lawyers to prioritize their caseloads and allocate resources more efficiently[16].

C. Document Review and Discovery

AI-driven document review and discovery platforms automate the process of reviewing and analyzing documents for relevance, privilege, and responsiveness in litigation. These platforms leverage machine learning algorithms to classify and categorize documents, identify key information, and streamline the review process. Key applications include:

AI-powered e-discovery platforms enable lawyers to efficiently process and review large volumes of electronic documents, emails, and other digital evidence in litigation[17].AI algorithms cluster documents based on similarities in content, enabling users to identify related documents and prioritize review efforts.AI tools automatically extract keywords and key phrases from documents, facilitating faster and more accurate search and retrieval of relevant information.

D. Sentencing Recommendations

Some jurisdictions have implemented AI-based systems to assist judges in determining appropriate sentences for criminal defendants. These systems analyze factors such as the defendant's criminal history,

[14]American Bar Association.(n.d.). Ethical and Professional Implications of Artificial Intelligence in Law Practice. Retrieved from https://www.americanbar.org/groups/science_technology/publications/
[15]Berkman Klein Center for Internet & Society at Harvard University.(2021). Principles for Building Responsible AI for Justice. Retrieved from https://cyber.harvard.edu/story/2021-08/principles-building-responsible-ai-justice
[16]Robotics and the Lessons of Cyberlaw" by Woody Hartzog and Neil M. Richards (2012)
[17]Super intelligence: Paths, Dangers, Strategies" by Nick Bostrom (2014)

demographics, and offense characteristics to generate sentencing recommendations. Key applications include:

AI algorithms assess the likelihood of recidivism and other risk factors associated with individual defendants, providing judges with information to inform sentencing decisions.AI systems aim to promote fairness and equity in sentencing by providing judges with objective, data-driven information about defendants' backgrounds and circumstances[18]. AI sentencing systems strive to be transparent and accountable by providing explanations for their recommendations and allowing for judicial review and oversight.

E. Virtual Legal Assistants and Chatbots

AI-powered virtual assistants and Chatbots provide individuals with legal guidance, automate routine tasks, and assist with legal issues through conversational interfaces. These tools leverage natural language understanding and dialogue management techniques to interact with users and provide personalized assistance. Key applications include:

Virtual legal assistants offer guidance on legal rights, responsibilities, and procedures, helping individuals navigate legal issues such as contracts, landlord-tenant disputes, and traffic tickets.AI chatbots automate the preparation of legal documents, such as contracts, wills, and lease agreements, by guiding users through the document creation process and generating customized templates. Virtual legal assistants assess the merits of legal claims and provide preliminary evaluations of potential legal issues, enabling individuals to determine the viability of pursuing legal action[19].These AI technologies offer significant opportunities to enhance the efficiency, accuracy, and accessibility of the legal system, while also raising important ethical and regulatory considerations that must be addressed to ensure responsible and equitable use.

IV. Benefits of AI Adoption in the Courtroom

A. Enhanced Efficiency and Productivity[20]

AI adoption in the courtroom leads to enhanced efficiency and productivity through automation and streamlining of various processes. Some specific benefits include:

1. *Automated Legal Research:* AI-powered legal research platforms can quickly analyze vast amounts of legal data, statutes, and case law to provide relevant information, saving lawyers and judges significant time and effort.

[18] Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy" by Cathy O'Neil (2016)

[19]Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World" by Bruce Schneier (2015)

[20]Big Data, Big Analytics: Emerging Business Intelligence and Analytic Trends for Today's Businesses" by Michael Minelli, Michele Chambers, and Ambiga Dhiraj (2012)

2. *Document Review Automation*: AI-driven e-discovery tools automate the review and analysis of documents, reducing the need for manual review and enabling legal teams to focus on higher-value tasks.

3. *Streamlined Case Management:* AI technologies facilitate better organization and management of case files, schedules, and deadlines, ensuring that legal proceedings progress smoothly and efficiently.

B. Cost Reduction and Resource Optimization[21]

AI adoption in the courtroom can lead to cost reduction and optimization of resources, benefiting both legal practitioners and court systems. Some key advantages include:

1. *Reduced Legal Research Costs:* AI-powered legal research platforms offer cost-effective solutions for accessing legal information, reducing the need for expensive subscriptions and manual research.

2. *Efficient Document Review:* AI-driven e-discovery tools streamline the document review process, minimizing the need for extensive manual review by legal professionals and reducing associated costs.

3. *Optimized Resource Allocation:* AI technologies enable more efficient allocation of human and financial resources by identifying priorities, allocating tasks, and optimizing workflows.

C. Improved Decision-making and Case Outcomes

AI adoption in the courtroom can improve decision-making and enhance case outcomes by providing access to relevant information, insights, and predictive analytics. Some key benefits include:

1. *Data-driven Decision-making:* AI technologies provide judges, lawyers, and litigants with access to data-driven insights and predictive analytics, enabling informed decision-making based on objective evidence and analysis.

2. *Enhanced Case Assessment:* AI-powered predictive analytics tools can assess the strengths and weaknesses of legal claims, predict case outcomes, and identify optimal legal strategies, leading to more favorable case outcomes.

3. *Consistency and Fairness:* AI technologies can help promote consistency and fairness in judicial decisions by reducing bias, increasing transparency, and ensuring that decisions are based on relevant legal principles and precedents.

D. Access to Justice and Legal Aid

[21]World Economic Forum. (2021). The Responsible Use of Technology - A Toolkit for Legal Professionals. Retrieved from https://www.weforum.org/reports/the-responsible-use-of-technology-a-toolkit-for-legal-professionals/

AI adoption in the courtroom can improve access to justice and legal aid by making legal services more affordable, accessible, and efficient. Some key advantages include:

1. *Virtual Legal Assistance:* AI-powered virtual legal assistants and Chatbots provide individuals with access to legal guidance, information, and resources, enabling them to navigate legal issues more effectively and affordably.

2. *Remote Court Proceedings:* AI technologies facilitate remote court proceedings, enabling individuals to participate in hearings and trials without the need for physical presence, reducing barriers to access to justice.

3. *Efficient Case Resolution:* AI technologies streamline legal processes, reduce delays, and expedite case resolution, ensuring that individuals have timely access to justice and legal remedies.

Overall, the adoption of AI in the courtroom offers significant benefits, including enhanced efficiency and productivity, cost reduction and resource optimization, improved decision-making and case outcomes, and increased access to justice and legal aid. However, it is essential to address challenges such as bias, transparency, and ethical considerations to ensure that AI technologies are deployed responsibly and equitably in the legal system.

V. Challenges and Limitations of AI in Legal Context

A. Bias and Fairness Concerns

One of the primary challenges associated with AI in the legal context is the potential for bias and fairness concerns. AI algorithms are trained on historical data, which may reflect systemic biases present in the legal system. As a result, AI systems may perpetuate and amplify existing biases, leading to unfair outcomes for certain individuals or groups. Key issues include:

1. *Data Bias:* AI systems may learn from biased or incomplete datasets, leading to skewed or discriminatory outcomes. For example, historical disparities in sentencing decisions may be reflected in AI-generated sentencing recommendations[22].

2. *Algorithmic Bias:* The design and implementation of AI algorithms may introduce bias, consciously or unconsciously, through factors such as feature selection, model parameters, and training methodologies.

[22]European Commission, "White Paper on Artificial Intelligence- A European approach to excellence and trust", 2020.

3. *Fairness and Equity:* AI systems must be designed to prioritize fairness and equity in decision-making, taking into account factors such as disparate impact, procedural justice, and distributive justice.

B. Data Privacy and Security Risks

AI adoption in the legal context raises significant data privacy and security risks, particularly concerning the collection, storage, and use of sensitive legal information. Key challenges include:

1. *Confidentiality Concerns:* Legal documents and communications contain highly sensitive and confidential information, raising concerns about unauthorized access, disclosure, or misuse of data.

2. *Data Breaches:* AI systems may be vulnerable to data breaches and cyberattacks, exposing sensitive legal information to unauthorized third parties and compromising privacy and confidentiality.

3. *Regulatory Compliance:* AI applications in the legal context must comply with data protection regulations and legal ethics rules governing the handling of confidential information, such as attorney-client privilege and the duty of confidentiality[23].

C. Lack of Transparency and Accountability

AI algorithms often operate as "black boxes," making it challenging to understand their decision-making processes and assess their reliability and accuracy. Lack of transparency and accountability in AI systems can undermine trust and confidence in the legal system. Key issues include:

1. *Opaque Decision-making:* AI-generated decisions may lack transparency, making it difficult to understand how decisions are reached and to challenge or appeal unfavorable outcomes[24].

2. *Accountability Gaps*: The complexity of AI systems and the division of responsibilities among developers, users, and regulators can create accountability gaps, making it unclear who is responsible for errors, biases, *or harms resulting from AI use.*

3. *Explain ability and Audibility:* AI systems must be designed to provide explanations for their decisions and actions, enabling users to understand the rationale behind AI-generated outcomes and to audit and validate AI processes for fairness and accuracy.

D. Ethical Dilemmas and Human Rights Implications

AI adoption in the legal context raises complex ethical dilemmas and human rights implications, particularly concerning issues such as autonomy, justice, and equality. Key concerns include:

[23]The Law Society, "Public Policy Commission on the use of Algorithms in the Justice System: Report" 2020.
[24]European Union Agency for Fundamental Rights. (2018).

1. *Legal Professional Ethics:* Lawyers and legal professionals must navigate ethical dilemmas related to the use of AI in legal practice, including conflicts of interest, competence, and the duty of loyalty to clients.

2. *Access to Justice*: AI technologies must be accessible to all individuals, regardless of socioeconomic status, linguistic proficiency, or technological literacy, to ensure equitable access to legal services and remedies.

3. *Human Rights Considerations:* AI systems must respect and protect fundamental human rights, including the right to a fair trial, the presumption of innocence, and due process, while also addressing challenges such as algorithmic discrimination and mass surveillance.

VI. Case Study

The Wisconsin Supreme Court upheld Loomis's conviction but acknowledged the potential biases and limitations of COMPAS. The court emphasized the importance of judicial discretion and transparency in sentencing decisions involving AI algorithms. The case highlighted the need for careful scrutiny of AI tools used in the criminal justice system and raised concerns about fairness, accountability, and the protection of defendants' rights[25].

In another case the Canadian Supreme Court considered the admissibility of evidence obtained through the use of an AI-based algorithm to analyze digital images of child pornography. The algorithm, known as CEDAR (Computerized Enhancement Detection and Reconstruction), was used by law enforcement to identify and categorize illegal images based on their content. The court ruled that evidence obtained through the use of CEDAR was admissible, but emphasized the importance of ensuring the reliability and accuracy of AI technologies used in criminal investigations. The case highlighted the potential benefits and risks of AI in law enforcement and underscored the need for robust standards and safeguards to protect privacy rights and prevent miscarriages of justice[26].

The California Supreme Court considered the use of AI algorithms in bail and pretrial detention decisions. The case challenged the legality of using risk assessment tools to determine bail amounts and detention conditions based on factors such as the defendant's criminal history, demographics, and offense characteristics. The court ruled that while risk assessment tools could be used as one factor in bail and pretrial detention decisions, they could not be the sole determinant. The case emphasized the need for judicial discretion, individualized assessments, and procedural safeguards in pretrial decision-making

[25]United States v. Loomis:2017
[26]R. v. N.F 2016

involving AI algorithms. It also raised concerns about the potential for bias, discrimination, and infringement of defendants' rights in the use of AI tools in the criminal justice system[27].

These case studies illustrate the complex legal and ethical issues surrounding the use of AI in the judicial system, including concerns about fairness, transparency, accountability, privacy, and due process. They underscore the importance of thoughtful regulation, oversight, and judicial review to ensure that AI technologies are used responsibly and ethically in legal proceedings.

VII. Ethical Considerations in AI-driven Judgments

A. Algorithmic Accountability and Transparency:

Algorithmic accountability and transparency are essential ethical considerations in AI-driven judgments. It is crucial to ensure that AI algorithms used in legal contexts are transparent, explainable, and subject to scrutiny. Key considerations include:

1. *Explain ability:* AI algorithms should be designed to provide clear explanations for their decisions and actions, enabling users to understand the rationale behind AI-driven judgments[28].
2. *Transparency:* The design, development, and deployment of AI algorithms should be transparent and subject to independent audit and review to ensure accountability and trustworthiness.
3. *Accountability:* Developers, users, and stakeholders should be held accountable for the decisions and outcomes resulting from AI-driven judgments, with clear mechanisms for redress and remediation in cases of errors or harms.

B. Fairness and Bias Mitigation Strategies:

Fairness and bias mitigation are critical considerations in AI-driven judgments to ensure equitable treatment and outcomes for all individuals. It is essential to address biases in AI algorithms and decision-making processes to prevent discrimination and uphold principles of fairness and justice. Key strategies include:

1. *Bias Detection:* AI algorithms should be tested and evaluated for biases based on factors such as race, gender, ethnicity, and socioeconomic status to identify and mitigate potential sources of unfairness.

[27]People v. Superior Court (Felmann) 1976
[28]The Ethical Algorithm: The Science of Socially Aware Algorithm Design" by Michael Kearns and Aaron Roth (2019)

2. *Fairness-aware Algorithms:* AI algorithms should be designed to prioritize fairness and equity in decision-making, taking into account factors such as disparate impact, procedural justice, and distributive justice[29].

3. *Bias Correction:* Techniques such as data preprocessing, feature engineering, and algorithmic adjustments can be used to correct biases in AI algorithms and ensure that decision-making processes are fair and unbiased.

C. Human Oversight and Intervention:

Human oversight and intervention are essential safeguards in AI-driven judgments to ensure accountability, oversight, and ethical decision-making. While AI algorithms can automate certain tasks and processes, human judgment and discretion remain crucial in complex legal contexts. Key considerations include:

1. *Human-in-the-loop Systems:* AI systems should incorporate mechanisms for human oversight and interventions, enabling human experts to review, validate, and intervene in AI-driven judgments when necessary.

2. *Human Oversight Committees:* Independent oversight committees or regulatory bodies can provide oversight and review of AI algorithms and decision-making processes, ensuring accountability and ethical compliance[30].

3. *Ethical Training and Education:* Legal professionals and decision-makers should receive training and education on the ethical implications of AI-driven judgments, including the importance of human oversight and intervention in ensuring fairness, transparency, and accountability.

D. Legal and Regulatory Frameworks:

Legal and regulatory frameworks play a crucial role in governing the use of AI in legal contexts and ensuring compliance with ethical principles and standards. Key considerations include:

1. *Regulatory Oversight:* Governments and regulatory bodies should establish clear guidelines, standards, and regulations governing the design, development, and deployment of AI algorithms in legal proceedings.

2. *Ethical Guidelines:* Professional associations, industry organizations, and academic institutions should develop ethical guidelines and best practices for the responsible use of AI in legal contexts, including considerations of fairness, transparency, and accountability.

[29]Big Data, Big Analytics: Emerging Business Intelligence and Analytic Trends for Today's Businesses" by Michael Minelli, Michele Chambers, and AmbigaDhiraj (2012)
[30]The Master Algorithm: How the Quest for the Ultimate Learning Machine Will Remake Our World" by Pedro Domingos (2015)

3. *Legal Protections:* Legal protections should be in place to safeguard individuals' rights and liberties in the use of AI-driven judgments, including protections against discrimination, privacy violations, and due process violations.

By prioritizing algorithmic accountability, fairness, human oversight, and regulatory compliance, stakeholders can ensure that AI technologies are used responsibly and ethically in legal proceedings, upholding principles of justice, fairness, and human rights.

VIII. Future Directions, Implications and Recommendations

A. Emerging Trends in AI and Law

As AI technologies continue to advance, several emerging trends are likely to shape the future of AI in the legal profession. Some key trends include:

1. *Natural Language Processing (NLP) Advancements:* Continued advancements in NLP technologies will enable AI systems to better understand and analyze complex legal texts, leading to more accurate legal research, document review, and case analysis.

2. *Explainable AI (XAI):* The development of explainable AI techniques will enhance transparency and accountability in AI-driven judgments by providing clear explanations for AI decisions, enabling users to understand and challenge AI-generated outcomes.

3. *Ethical AI Design:* There will be a growing emphasis on ethical AI design principles, including fairness, transparency, accountability, and human oversight, to ensure that AI technologies are deployed responsibly and ethically in legal contexts.

4. *Interdisciplinary Collaboration:* Collaboration between legal professionals, data scientists, ethicists, and policymakers will become increasingly important to address the complex ethical, legal, and societal implications of AI in the legal profession.

B. Potential Impact on Legal Profession

The widespread adoption of AI in the legal profession will have profound implications for legal practitioners, law firms, and the broader legal ecosystem. Some potential impacts include:

1. *Transformation of Legal Practice:* AI technologies will automate routine legal tasks, such as legal research, document review, and contract analysis, allowing legal professionals to focus on higher-value tasks requiring human judgment and expertise.

2. *Changes in Legal Education:* Legal education programs will need to incorporate training in AI technologies, data analytics, and computational thinking to prepare future lawyers for the evolving demands of the legal profession.

3. *New Legal Roles and Specializations:* AI adoption will create new opportunities for legal professionals to specialize in areas such as AI ethics, data privacy, cyber security, and technology law, reflecting the increasing intersection of law and technology.

4. *Shift in Client Expectations:* Clients will increasingly expect legal services to leverage AI technologies to deliver faster, more efficient and cost-effective solutions, driving law firms to adopt AI tools and capabilities to remain competitive.

C. Policy Recommendations and Guidelines

To ensure the responsible and ethical use of AI in the legal profession, policymakers, regulators, and industry stakeholders should consider implementing the following policy recommendations and guidelines:

1. *Regulatory Oversight:* Governments should establish clear regulatory frameworks governing the design, development, and deployment of AI technologies in legal contexts, including standards for transparency, fairness, accountability, and data privacy.

2. *Ethical Guidelines:* Professional associations and industry organizations should develop ethical guidelines and best practices for the responsible use of AI in legal practice, including considerations of bias mitigation, human oversight, and algorithmic transparency.

3. *Education and Training:* Legal education programs should incorporate training in AI technologies, data analytics, and ethical AI design principles to prepare future lawyers for the ethical and practical challenges of integrating AI into legal practice.

4. *Research and Development Funding:* Governments, foundations, and industry partners should invest in research and development initiatives focused on advancing AI technologies and methodologies that prioritize ethical considerations and societal impact.

By promoting transparency, accountability, fairness, and human oversight, stakeholders can ensure that AI technologies contribute to the advancement of justice, fairness, and the rule of law.

IX. Conclusion

In conclusion, the integration of artificial intelligence (AI) into the judicial system presents both opportunities and challenges. AI technologies have the potential to enhance efficiency, productivity, and decision-making in legal proceedings, leading to improved access to justice and legal aid. However, the

widespread adoption of AI in the courtroom also raises ethical, legal, and societal concerns that must be addressed to ensure responsible and equitable use.

Ethical considerations, such as algorithmic transparency, fairness, and bias mitigation, are paramount in AI-driven judgments to uphold principles of justice, fairness, and human rights. It is essential to prioritize human oversight and intervention, ensuring that AI systems operate transparently and accountably while preserving the discretion and judgment of legal professionals.

Moreover, legal and regulatory frameworks must adapt to the challenges posed by AI technologies, providing clear guidelines and standards for the design, development, and deployment of AI systems in legal contexts. Collaboration between legal experts, technologists, policymakers, and ethicists is crucial to navigate the complex ethical and legal issues arising from AI integration in the judicial system.

Ultimately, the responsible and ethical use of AI in the courtroom requires a multidisciplinary approach that balances technological innovation with ethical considerations, legal principles, and societal values. By addressing these challenges and leveraging the potential of AI technologies responsibly, stakeholders can harness the benefits of AI to advance justice, fairness, and the rule of law in the digital age.

Distributed Ledger Technology and the Reserve Bank of India

PRITAM KUMAR

Pritam Kumar is currently a fifth year law student at National University of Study and Research in Law , Ranchi, Jharkhand

Abstract

The features and complexity of Distributed Ledger Technology have grown significantly to provide solutions to various industries, including the financial sector. Some central banks have launched pilot projects to study and comprehend DLT, as well as to investigate the potential benefits for their operations and financial systems. So far, most of these projects have been exploratory, examining the viability of conducting inter-bank settlements, settlement of digital assets and tokens, and cross-border payments across DLT platforms using existing system functionalities. In the Indian context, increasing support for innovations and emerging technologies from the Reserve Bank of India and the Government of India through regulatory spaces and other schemes would pave the way for the new economy, enriched with the momentum of technology-centric growth.

I. Introduction

The broad term used to describe techniques for managing distributed ledgers over computer networks is "DLT." A purist (or perhaps a pedant) would point out that although "blockchain" is frequently used as a synonym for "DLT" , Blockchain is a form of distributed ledger technology which has distinct features among other types of DLTs. There are other types of DLT that are not based on blockchain technology, however many of the more well-known examples are. It is a digital document that is instantly distributed across a group of participants. It is distributed because every user (or node) in the network has a copy of the record, and each copy receives updates at the same time. Different distributed ledger platforms employ a variety of consensus techniques to ensure that all nodes concur on the record. One major benefit of DLT is that there is just one set of records, even though it is

maintained on various nodes, rather than several competing ones that need to be reconciled. This one record is a prime source of information[1].

A blockchain is a globally shared, transactional database. This means that everyone can read entries in the database just by participating in the network. If you want to change something in the database, you create a so-called transaction which is required to be accepted by all others. The word transaction implies that the change you want to make (assume you want to change two values at the same time) is either not done at all or completely applied. Furthermore, while your transaction is applied to the database, no other transaction can alter it. As an example, imagine a table that lists the balances of all accounts in an electronic currency. If a transfer from one account to another is requested, the transactional nature of the database ensures that if the amount is subtracted from one account, it is always added to the other account[2]. If due to whatever reason, adding the amount to the target account is not possible, the source account is also not modified. Furthermore, a transaction is always cryptographically signed by the sender (creator). This makes it straightforward to guard access to specific modifications of the database. In the example of the electronic currency, a simple check ensures that only the person holding the keys to the account can transfer money from it[3].

Out of the wreckage of the global financial crisis (GFC) arose a white paper titled 'Bitcoin: A Peer-To-Peer Electronic Cash System' (Nakamoto, 2008), which provided a roadmap for revolutionizing the financial system. Since then, the world has rapidly evolved from Bitcoin and early blockchain designs to customized blockchains tailored to the needs of various industries. There are currently over 2,000 cryptocurrencies1 listed on major cryptocurrency exchanges, as well as numerous blockchain startups around the world. Blockchain has become a buzzword, and no FinTech discussion is complete without mentioning it. Such growth in popularity over a decade reflects the inherent revolutionary features of blockchain and its appeal to technically insightful entrepreneurs.

II. Why utilize DLTs?

FinTech companies that provide solutions for remittances and international payments based on blockchain technology are quickly upending and challenging market players. In order to lower risk, avoid fraud, and better implement monetary policy, central banks and other authorities are increasingly understanding that they could profit from this technology (De Meijer, 2018). As a result,

[1] Nalin Priyaranjan, Dr. Mohua Roy and Dr. Sarat Dhal of the Department of Economic and Policy Research (DEPR), Reserve Bank of India, 'Distributed Ledger Technology, Blockchain and Central Banks' (2020) <https://rbidocs.rbi.org.in/rdocs/Bulletin/PDFs/03AR_11022020510886F328EB418FB8013FBB684BB5BC.PDF > accessed 23 October 2024

[2] Nalin Priyaranjan, Dr. Mohua Roy and Dr. Sarat Dhal of the Department of Economic and Policy Research (DEPR), Reserve Bank of India, 'Distributed Ledger Technology, Blockchain and Central Banks' (2020) <https://rbidocs.rbi.org.in/rdocs/Bulletin/PDFs/03AR_11022020510886F328EB418FB8013FBB684BB5BC.PDF> accessed 23 October 2024

[3] 'What is Blockchain?' (*McKinsey & Company*, 6 June 2024) <https://www.mckinsey.com/featured-insights/mckinsey-explainers/what-is-blockchain> accessed 21 October 2024

some central banks have set out on an ambitious journey to support and steer the sector in a non-disruptive manner, maintain financial stability, and guarantee the growth of financial market infrastructure using DLT[4]. There seems to be a substantial lack of knowledge regarding blockchain and DLT despite the public's intense interest in these new technologies. Due to the complexity of this technology and the numerous regulatory challenges it presents, including "the fast-moving vocabulary around blockchain technology and the challenges this unstable verbal terrain poses for regulators," several central banks and other regulatory authorities have been cautious in adopting it. Consider the adage of Charles Kettering that "a problem adequately expressed is half remedied" in this situation. This study is driven by the need to provide a clear knowledge of DLT, blockchain, and the applications of these technologies by central banks; the lessons learned from this study may also be applicable to the Indian context.

Legitimate ownership of items like homes, automobiles, and other possessions is established by a tangible document that is accepted by the general public and issued by an authorized institution. The verification procedure and the prevalence of fake certificates are two of the main problems with this type of ownership proof[5]. Every account in the distributed ledger technology (DLT) includes a digital public key and private key pair that are used to sign and encrypt blocks using hashing algorithms. The DLT structure's framework is composed of this mechanism. Here, the ownership information is recorded in a publicly accessible electronic ledger that uses cryptography to prevent tampering. The usage of a private key, which is used to sign transactions and so provide proof that it came from the owner and can be easily checked by using its public key pair, ensures the validity of transactions. Recent DLT Issues and Developments from Satoshi Nakamoto's paper from 2008, which served as the foundation for blockchain, it has come a long way. Although the first use of it was for cryptocurrencies, other uses have recently gained popularity. Limited uses, sluggish transaction confirmation, low throughput, lack of privacy, and high energy consumption are only a few of the initial drawbacks of the first generation of blockchains. These New approaches like sharing, alternative consensus mechanisms like Proof-of-Stake, and permissioned blockchains for specific applications, like wholesale interbank settlements (Proof-of-Concept projects by the Bank of Canada and Monetary Authority of Singapore), are being used to address shortcomings. Blockchain interoperability is being developed for cross-platform functionality. Other DLT systems, such as Quorum Corda, Hyperledger, etc., have been developed as a result of rising demand for various solutions[6].

III. Permissioned versus Permissionless DLT

[4] Rodrigo Mejia Ricart & Camilo Tellez, 'Distributed Ledger Technology: What is it and why Do we care' (*Better than cash Alliance*, 6 June 2019)<https://www.betterthancash.org/news/distributed-ledger-technology-what-is-it-and-why-do-we-care > accessed 18 October 2024
[5] Mohd Javaid, Abid Haleem & Ravi Pratap Singh, 'A review of Blockchain Technology applications for financial services' (July 2022) <https://www.sciencedirect.com/science/article/pii/S2772485922000606> accessed 20 October 2024
[6] Dr. Mushtaq Ahmed, 'Blockchain Technology' <https://egovstandards.gov.in/sites/default/files/2023-05/Blockchain%20Cryptographic%20Security%2C%20Hashing%20and%20Digital%20Signature.pdf> accessed 22 October 2024

A DLT can be categorized as permissioned (requiring prior authorization to join) or permissionless based on its capacity to authenticate transactions (anyone can participate). Most first-generation blockchains, including Bitcoin and Ethereum, lack permissions. Systems using permissionless DLT are extremely transparent since everyone can see every transaction recorded on the ledger. They take a long time to use, though, and are not appropriate for solutions that demand transaction privacy. Permissioned DLT platforms were launched for a controlled environment where participants trust each other and privacy is based on governance decisions. Select agents are given access to validate transactions by nature. DLT can be constructed so that an agent can only access its own transactions and not those of other agents, satisfying the privacy requirements. Business and financial agents have this as a key requirement[7].

IV. Smart Contracts

Smart Contracts are essentially self-executing pieces of business logics that mediates a specific transaction on the blockchain with pre-defined scripts contained within the code of the transaction[8]. This code autonomously controls the execution of the contract and ensures transactions are trackable and irreversible. These contracts are essentially DLT lines of code or logic that run on their own when certain prerequisites are satisfied. These can be thought of as digital contracts, and when the conditions are met, the smart contract verifies them and transfers the tokens in accordance with the conditions (Buterin, 2013). A straightforward smart contract would automatically split and send payments to the designated parties after being received. A smart contract's ability to communicate with other smart contracts allows it to become more complicated. In numerous central bank and other institution pilot programs, smart contracts have been used in services including trade financing, settlement of securities, etc[9].

V. Blockchain Interoperability

[7] Toshendra Kumar Sharma, 'Permissioned and Permissionless Blockchains: A Comprehensive Guide' (10 May 2024) <https://www.blockchain-council.org/blockchain/permissioned-and-permissionless-blockchains-a-comprehensive-guide/ > accessed 26 October 2024
[8] <https://www.ibm.com/topics/smart-contracts> accessed on 25 October 2024
[9] Shafaq Naheed Khan, 'Blockchain Smart Contracts: Applications, challenges and future trends'(18 April 2021) <https://link.springer.com/article/10.1007/s12083-021-01127-0> accessed 24 October 2024

There are numerous active blockchain and DLT platforms worldwide. These DLT platforms can communicate with one another to deliver required services and are designed for certain use cases. This DLT property is sometimes contrasted with the Internet, a network of networks. According to interoperability, if one transaction takes place on one DLT platform, another transaction will presumably follow on a separate DLT platform. Project Jasper and Project Ubin from the Monetary Authority of Singapore and the Bank of Canada respectively show the value of such interoperability in cross-border payment operations (Bank of Canada et al, 2018)[10].

VI. DLT and Blockchain Platforms

DLT and blockchains should be seen as platforms for creating more complex applications rather than just ways to move currency. By design, every DLT platform is distinct, with a distinct set of capabilities, benefits, and drawbacks. Choosing the appropriate platform for the application at hand is crucial. The timeline shows the evolution of these platforms beginning with Bitcoin.

VII. DLT in Central Banks

Blockchain became well-known thanks to the cryptocurrency Bitcoin. Central banks all over the world started to keep an eye on the threats posed by cryptocurrencies since it was encroaching on the territory of the central bank, which is the sole issuer of currency in an economy. Central banks showed confidence and interest in blockchain-based applications other than cryptocurrencies while keeping an eye on these developments. The World Economic Forum (WEF) released a paper titled "The future of financial infrastructure" in August 2016 that included information on the potential ways that blockchain technology could transform financial services with uses spanning from payments to equity settlements.

Central banks realized they could support innovations in a quickly changing digital context after being given the task of creating financial infrastructure. It was also recognized that central bank participation might increase the security and stability of these platforms and boost the efficiency of the financial industry as a result. Bank of Canada and the Monetary Authority of Singapore recently tested cross-border payments on their respective blockchain networks as part of their programs. As Facebook's

[10] Nalin Priyaranjan, Dr. Mohua Roy and Dr. Sarat Dhal of the Department of Economic and Policy Research (DEPR), Reserve Bank of India, 'Distributed Ledger Technology, Blockchain and Central Banks' (2020) <https://rbidocs.rbi.org.in/rdocs/Bulletin/PDFs/03AR_11022020510886F328EB418FB8013FBB684BB5BC.PDF> accessed 23 October 2024

intended launch of Libra was revealed in a white paper in June 2019, the interest of central banks in DLT increased further in the second half of 2019.

Several central banks have started projects (Annex) over the past five years to research and test DLT technology in order to evaluate its potential for use in financial infrastructure. The majority of the initiatives have an exploratory goal rather than a replacement goal for the current financial infrastructure, which is to examine whether current systems are still viable on a new decentralized platform. These initiatives are largely designed to increase central banks' awareness of DLT and investigate the viability of gradually integrating CBDC into the financial system.

Applications of DLT in India Following Bitcoin, several cryptocurrency firms have emerged in India, including Uno coin in 2013 and Zebpay in 2014. (Tracxn, 2019). However, the price volatility of Bitcoin and the fraud cases have highlighted regulatory worries about the dangers of cryptocurrencies. Both the Reserve Bank and the Government of India have said that they have not authorized or issued regulations for any institution to deal with cryptocurrencies. As a result, individuals dealing with cryptocurrencies have no legal protection and are responsible for any associated risks.

In truth, the Reserve Bank has warned against trading in cryptocurrencies in a number of news statements (Dec 24, 2013, Feb 1, 2017, Dec 5, 2017). The Reserve Bank forbade its regulated entities from providing their services to businesses dealing with cryptocurrencies or virtual currencies in April 2018 through a circular dated 6th april,2018 in order to protect domestic depositors and financial institutions from the rising risks brought on by speculative dealings in cryptocurrencies. But In the case of *Internet And Mobile Association of India v. Reserve Bank Of India, MANU/SC/0264/2020,* The Supreme Court of India declared the said circular unenforceable.

The authorities have, however, acknowledged the value of DLT and blockchain. In light of this, it is essential for Indian institutions to comprehend the potential advantages and risks of DLT in order to benefit from technological progress. The adoption of DLT and blockchain in India has advanced recently in both the public and private sectors, despite the fact that the majority of the initiatives are still in the proof-of-concept stage. In actuality, blockchain-based solutions are becoming increasingly popular in the public sector. In the fields of property registry, digital certificates, electronic health records, and other sectors, certain state governments, including those of Andhra Pradesh and Telangana, have begun implementing blockchain-related solutions (Government of Andhra Pradesh September 2018).

The private sector's adoption of blockchain-based solutions is being led by the banking and financial services industry. These initiatives serve as examples, with some of them being Yes Bank's implementation of the issuance of commercial papers on blockchain (Yes Bank, July 2019), Axis Bank's launch of an international payment service using Ripple's enterprise blockchain technology (Axis Bank, November 2017), and the execution of a blockchain-based trade finance transaction by HSBC India and Reliance Industries Ltd. (HSBC India, November 2018). Startups are using blockchain technology to

offer solutions in a variety of sectors, including healthcare, retail, government services, and human resources. Around US$ 8.5 million has reportedly been invested by venture capitalists in blockchain-based firms in India (NASSCOM, 2019).

However, according to this analysis, Indian start-ups were only able to secure 0.2% of the surge in venture capital investments in blockchain startups around the world. Through its new regulatory sandbox environment, the Reserve Bank of India has been proactive in offering advice for the development of blockchain-based applications. Startups and financial institutions that use blockchain-based applications may be added to regulatory sandbox cohorts to test their products for a predetermined amount of time. Recently, the Government of India announced a number of initiatives in the Union Budget 2020–21, focusing on the new economy built on cutting-edge technologies like artificial intelligence, machine learning, the Internet of things, etc.

The National Mission on Quantum Technologies and Applications was given 8,000 crores over a five-year period, and 6,000 crores for improving digital connectivity at the grass-root level by connecting 1 lakh Gram Panchayats under the Bharatnet program. It was also proposed to release a policy allowing the private sector to build Data Center parks across the nation. Additionally, it was suggested to postpone paying taxes on shares distributed by startups to their employees under employee stock option schemes (ESOPs). These initiatives would therefore create new investment and employment opportunities in addition to opening up new pathways for start-ups to develop and thrive. More start-ups and investments are anticipated as the regulatory framework surrounding DLT and blockchain technology develops with the introduction of a regulatory sandbox[11].

VIII. Conclusion

DLT and blockchain have grown significantly in features and complexity over the past ten years to provide solutions for many industries, including the financial sector. Due to their intricacy, DLT was initially only understood by computer scientists and a select few other curious people. However, there is a lot of interest in DLT since it has uses in finance and other industries. Pilot initiatives to research, comprehend, and investigate the possible advantages of DLT for their operations and the financial systems have been performed by some central banks in partnership with other organizations.

The majority of these initiatives are currently experimental in nature and study whether it is feasible to carry out cross-border payments using DLT platforms, inter-bank settlements, and the settlement of digital assets and tokens using the functions of the current system. It's crucial to keep in mind that the majority of these central banks haven't yet stated that they intend to launch DLT-based applications

[11] 'Budget 2020 announces Rs 8000 cr National Mission on Quantum Technologies & Applications' <https://dst.gov.in/budget-2020-announces-rs-8000-cr-national-mission-quantum-technologies-applications> accessed 26 October 2024

in production. The Riksbank, among other things, has indicated that DLT in its current form is too immature to be used for the deployment of e-krona, even in the case of CBDC. The Riksbank, has expressed concerns about DLT for the deployment of its e-krona, even though DLT has potential applications in central bank digital currencies (CBDCs) due to its scalability, performance limitations, regulatory uncertainty, energy consumptions and interoperability issues.

However, these initiatives and the benefits they provide strengthen the power of central banks and regulators to direct the construction of a DLT-based financial market infrastructure. As institutions and start-ups embark on adopting new technology to provide effective and efficient answers to business problems, this also enables central banks to offer helpful counsel.

In the Indian context, growing support for innovations and emerging technologies from the Reserve Bank of India and the Government of India through regulatory sandbox and several other initiatives will pave the way for a new economy enhanced with impetus for technology-centric growth.