**International Journal of Global Research Innovations & Technology (IJGRIT)**
ISSN : 2583-8717(Online), Impact Factor: 6.972, Volume 03, No. 03, July-September, 2025, pp 12-26

# A Systematic Review on Dark Patterns: Whisper in Clicks, Hide in Links

**Anjali Thukral[1] | Nidhi Aggarwal[2*] | Anusha Garg[3] | Lipika[4]**

[1,2,3&4]Keshav Mahavidyalaya, University of Delhi, Delhi, India.

*Corresponding Author: nidhi.aggarwal@keshav.du.ac.in

*Citation: Thukral, A, Aggarwal, N, Garg, A & Lipika. (2025). A Systematic Review on Dark Patterns: Whisper in Clicks, Hide in Links. International Journal of Global Research Innovations & Technology, 03(03),12–26. https://doi.org/10.62823/IJGRIT/03.03.7864*

## ABSTRACT

*Dark patterns are manipulative designs that hide deception behind visually appealing User Interface (UI) elements. They are incorporated into the UI, with the primary aim of gaining profit by manipulating the users psychologically and financially. Over the years, a substantial body of research has investigated the prevalence and impact of dark patterns across various digital platforms, including mobile applications, websites, and online games. These patterns manifest in various forms, including text, images, videos, and hyperlinks. This paper presents a Systematic Literature Review (SLR) of the most relevant and recent research on dark patterns. The review categorizes the literature across four key dimensions: types of dark patterns, UI features, detection techniques, and their associated limitations. Detection methods are further classified based on the algorithms employed, with BERT emerging as the most frequently used baseline model in these studies. Among the commonly identified dark patterns are Forced Action, Misdirection, Sneaking, Scarcity, and Obstruction. Findings suggest that Mathur's dataset, comprising information from 11K e-commerce websites, is the most widely utilized in the reviewed literature. Along with technological aspects, we examine government regulations and guidelines aimed at eliminating dark patterns. Therefore, our review enhances understanding and supports the development of dark pattern detection by helping emerging researchers create new and effective detection algorithms.*

***Keywords**: Dark Patterns, Manipulative Designs, Deceptive Designs, Detection Techniques, User Interface.*

## Introduction

Over the years, every domain has made its mark in the digital world, be it education, e-commerce, gaming, or socialising. People of all age groups now heavily rely on digital platforms, even for basic household purchases. This growing dependence on digital channels has raised serious concerns regarding user safety. To keep users engaged and increase profits, many platforms undertake many manipulative designs that bind the user's actions. These designs are named as dark patterns by Harry Brignull in 2010 (Brignull et al., 2023). Dark patterns are UI design choices that benefit an online service by coercing, steering, or deceiving users into making decisions that, if fully informed and capable of selecting alternatives, they might not make (Mathur et al., 2019). Such malicious interface designs are rapidly proliferating across various digital platforms (Conti & Sobiesk E, 2010), such as shopping websites (Dmitry & Yerkebulan, 2022; Mathur et al., 2019; Ramteke et al., 2024; Sazid & ENASE, 2024; Yada et al., 2023), mobile apps

(Chen J et al., 2023; Yue C et al., 2024), video games (Hadan et al., 2024; Mukherjee et al., 2025), chatbots (Kran et al., 2025; Traubinger et al., 2024), Extended Reality (XR) and Augmented Reality (AR) environments (Krauß et al., 2024; Meinhardt et al., 2025; Mukherjee et al., 2025). Dark patterns are widely used in businesses to trap visitors into accepting terms and conditions that are profitable to them (Bajaj et al., 2025). They are annoying and frequently affect user experience. In the worst cases, they can deceive and mislead users, resulting in financial loss, manipulation into revealing personal information, fostering compulsive or addictive behaviors in both adults and children (Mathur et al., 2019), playing malicious ads automatically (Mukherjee et al., 2025) and making it tough to cancel subscriptions (Gray et al., 2025).

About 76% of the sites and apps that offered subscription services across the globe have employed at least one possible dark pattern, while around 67% have incorporated multiple such patterns (FTC, 2024). Although the motivations for using dark patterns can vary, they typically focus on reaching specific objectives or results that benefit the organisation using them (Bajaj et al., 2025). Still, most users are unaware of these dark patterns that violate their privacy and use harmful tactics to control their actions. Therefore, dark patterns have emerged as a critical area of study due to their widespread presence and impact on user experience. The primary objective of this work is to evaluate the existing body of research on dark patterns. While numerous taxonomies and detection methods have been proposed, significant limitations still persist in accurately identifying and mitigating these deceptive design practices. This study presents a comprehensive review of 21 research papers to identify the most prominent dark patterns discussed in the literature and maps the detection techniques, including Machine Learning (ML), Deep Learning (DL), and custom frameworks. This research provides a holistic overview aimed at raising awareness about various types of dark patterns, summarizing current detection strategies, and highlighting areas for future research. This, in turn, underscores the importance of addressing dark patterns more seriously within both academic and user communities.

## Methodology

To identify relevant literature on dark patterns, we conducted a comprehensive and systematic search using two major academic databases: Google Scholar and Scopus. We used a combination of search queries, including (TITLE-ABS-KEY("dark patterns" OR "deceptive design", "dark patterns" AND "deceptive design", "dark patterns", and "dark patterns" OR "DP")), to leverage the advanced search tools provided by both platforms. All articles reviewed herein are obtained using the above query as of May 27, 2025. An overview of the PRISMA framework (Page et al., 2021) is provided in Figure 1.

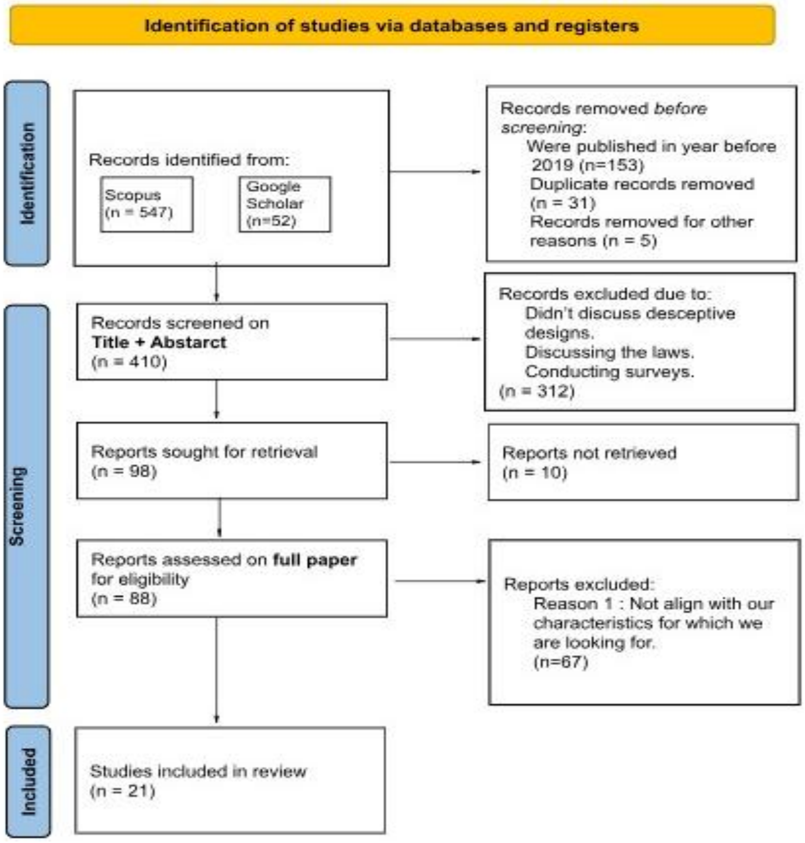
Identification of studies via databases and registers
Identification
Records identified from:
Scopus (n = 547)
Google Scholar (n=52)
Records removed before screening:
Were published in year before 2019 (n=153)
Duplicate records removed (n = 31)
Records removed for other reasons (n = 5)
Screening
Records screened on Title + Abstarct (n = 410)
Records excluded due to:
Didn't discuss desceptive designs.
Discussing the laws.
Conducting surveys.
(n = 312)
Reports sought for retrieval (n = 98)
Reports not retrieved (n = 10)
Reports assessed on full paper for eligibility (n = 88)
Reports excluded:
Reason 1 : Not align with our characteristics for which we are looking for.
(n=67)
Included
Studies included in review (n = 21)

**Figure 1: A systematic review using the PRISMA Framework**

This initial search yielded 52 results from Google Scholar and 547 from Scopus, giving 599 articles. To ensure quality and relevance, researchers applied several exclusion criteria, including removing duplicates, articles published before 2019, and eliminating papers that did not align with the scope of our study. After this filtering process, 410 articles were left. We then screened titles and abstracts to narrow the selection to 98 articles. A further detailed review of the key sections of each paper, focusing on the inclusion of datasets, types and features of dark patterns, and detection techniques, was conducted with the help of SciSpace[1]. Lastly, 21 full-length research articles that directly addressed our criteria were selected for final analysis. Our final corpus comprises studies published between 2019 and 2025, ensuring that the review reflects the latest trends in AI-based detection methods and modern UI design practices.

The following section presents a detailed review of the research studies, discussing the types, features, detection techniques, and datasets associated with dark patterns.

## Literature Review

This section is organized into three subsections: types of dark patterns, detection techniques, and datasets. Table 2 presents a summary of the types of dark patterns, the features extracted, the datasets utilized, the detection methods applied, and the associated limitations.

### Types of Dark Patterns

In 2010, (Brignull et al., 2023) introduced the first taxonomy of dark patterns based on his observations, though it lacked formal documentation. His classification primarily focused on web and software tricks designed to manipulate users into unintended actions. Later, Conti & Sobiesk E, (2010) proposed a taxonomy derived from a 12-month investigation encompassing desktop software, websites, and non-desktop interactions. To validate their framework, they surveyed 22 undergraduate students who actively identified harmful interface practices, along with a group discussion involving approximately 75 participants at the Hackers of Planet Earth Conference. In 2016, (Bösch et al., 2016) developed their taxonomy with a focus on human cognitive processes, analyzing popular websites and mobile apps for privacy-related manipulative patterns. Using a structured pattern template, they identified and described several recurring "dark privacy patterns."

In 2021, (Mathur et al., 2021) introduced a taxonomy structured around five dimensions: Asymmetric, Covert, Deceptive, Hides Information, and Restrictive. Their classification comprises 7 categories and 15 distinct types of dark patterns. Ahuja & Kumar J, (2022) conducted a normative evaluation of 151 dark patterns from 16 taxonomies, emphasizing user autonomy. The result was a synthesis of 25 dark strategies.

In 2023, (Gray et al., 2023) aimed to build a unified language for dark patterns by harmonizing ten regulatory and academic taxonomies. Their study proposed a three-level ontology with standard definitions for 64 dark pattern types, organized across low-level, meso-level, and high-level categories.

More recently, (Lewis & Vassileva, 2024)visualized the interrelationships among dark patterns by integrating various taxonomies into a directed graph, enabling cluster detection to reveal how patterns are interconnected. Over time, taxonomies of dark patterns have become increasingly structured, with researchers working toward more refined and hierarchical classifications. Figure 2 illustrates the most frequently identified types of dark patterns found in the literature. Certain patterns are particularly harmful, coercing users into actions against their intent. These are often labeled as privacy-specific (Potel-Saville & Da Rocha, 2024), high-level (Gray et al., 2023), or active dark patterns (Sazid & ENASE, 2024). In contrast, some patterns are more neutral in nature, exerting minimal impact on user behavior. Based on the review of existing taxonomies and scholarly classifications of dark patterns, the following table (Table 1) presents a systematic overview of prominent dark pattern types, along with their descriptions and practical examples.

**Table 1: Types of Dark Patterns**

| Dark Patterns | Description | Example |
|---|---|---|
| Nagging | Repeatedly asking users to perform an action they've already declined. | Constant popups asking to allow notifications. |
| Confirm shaming | Using guilt-tripping language to push users into opting in. | "No thanks, I hate saving money." |

[1] https://scispace.com/

| | | |
|---|---|---|
| Obstruction | Making a process harder than necessary to discourage a user action. | Difficult unsubscribe process from an email list. |
| Misdirection | Focusing user attention on one thing to distract from another. | Highlighting a "Yes" button and hiding the "No" option. |
| Sneaking / Sneak into Basket | Adding items to the cart or checkout without user consent. | E- commerce platforms automatically add a donation at checkout. |
| Urgency | Creating a false sense of urgency to pressure decisions. | "Only 1 room left!" on hotel booking websites. |
| Scarcity | Suggesting limited availability to manipulate choice. | "Only 2 items in stock – hurry!" |
| Forced Action | Forcing users to complete an unrelated task to proceed. | Must sign up for the newsletter to access a feature. |
| Hidden Costs | Extra charges and fees were revealed late in the process. | Adding delivery charges and platform fees at the end of the purchase process. |
| Interface Interference | Deliberately designing UI to mislead. | Tiny close buttons, big accept buttons for ads. |
| Bait and Switch | Promising one thing but delivering something else. | Clicking a "Free Download" button, but instead, it starts downloading unrelated software or redirects to a paid version. |
| Disguised Ads | Ads are presented as regular content or buttons. | Sponsored posts on social media that closely mimic organic content, with the "Ad" label barely visible. |
| Social Proof | Manipulates users by presenting exaggerated or fake cues about others' actions to pressure decisions. | Fake reviews or testimonials to simulate trust and popularity. |

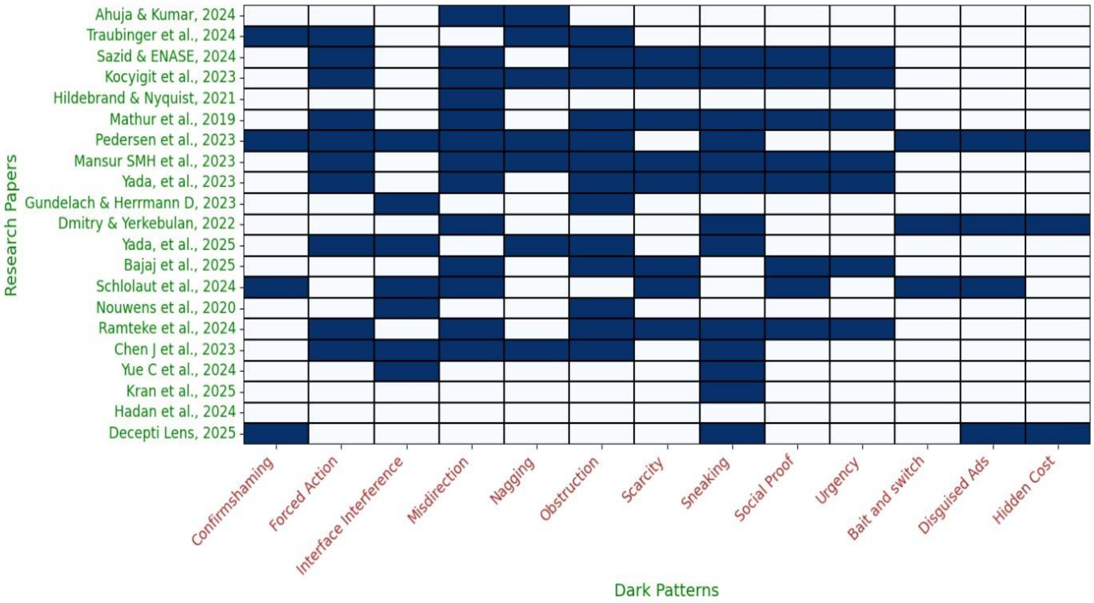

**Figure 2: Previous Research on Dark Patterns**

### Techniques

Researchers have used a wide range of techniques, as shown in Table 2. To understand and evaluate these techniques, we have categorised them into three primary tasks: data extraction and processing, classification and detection, and evaluation, which together comprise the entire dark pattern detection process.

## Table 2: Summary of Detecting Dark Patterns- Types, Features, Datasets, Techniques, and Limitations

| S.No. | Research Articles | Types | Features | Techniques | Limitations |
|---|---|---|---|---|---|
| 1 | (Ahuja & Kumar, 2024) | Nagging, Misdirection,<br>Hidden Information | Colors, Fonts, Call to Action, Layout, Navigation, Content, Choice, Social Influence, Architecture, Incentives<br>**Dataset**: 48 problematic design elements. | Layered Analysis of Persuasive Designs | The corpus is not exhaustive. Newer design elements can be added to this corpus. |
| 2 | (Traubinger et al., 2024) | Nagging, Confirmshaming, Hard to Cancel, Forced Action, Obstruction, Usability Smells | Text<br>**Dataset:** ChIPS dataset with 69 complaints from different web sources (GitHub - Vertr/ChIPS-Dataset, 2024). | Analysed users' complaints and usability issues in the chatbots.<br>These complaints were then classified. | Subjective reporting, coder bias, small dataset, over-attributing problems |
| 3 | (Sazid & ENASE, 2024) | Social Proof, Urgency,<br>Scarcity, Sneaking,<br>Forced Action, Obstruction,<br>Misdirection | Text<br>**Dataset:** It contains 99 dark pattern texts extracted from 131 e-commerce websites in Bangladesh (GitHub - Yasin-Sazid/Dark-Patterns-Bangladesh, 2024). | Page segmentation algorithm, Robustly Optimized BERT Approach (RoBERTa) and Generative Pretrained Transformer 3 (GPT-3) | The automated detection approach may have missed some dark pattern data as false negatives. |
| 4 | (Kocyigit et al., 2023) | Sneaking, Urgency,<br>Misdirection, Social Proof, Scarcity,<br>Obstruction, Forced Action, Nagging<br>Interface Inference | Cookie consent flow<br>**Dataset:** It Contain 10 different websites | Unified Modeling Language (UML) activity diagrams | Analysis limited to 10 websites. Visual elements, request detection and content extraction from cookies were not considered. Features unable to describe examples that exploit human emotions. |
| 5 | (Hildebrand & Nyquist, 2021) | Nudging towards acceptance, Privacy Zuckering, Misdirection, Trick Question | Size of notice, Size of buttons, Comparing button color, Amount of pre-ticketed boxes, Readability, How long does the site save cookies? Does the site redirect the user when rejecting cookies?<br>**Dataset**: Top 10 million websites taken from the Open PageRank Initiative[1] | Automatic analyzer | Ineffective at easily identifying the button that a user finds most visually appealing. |
| 6 | (Mathur et al., 2019) | Social Proof, Urgency,<br>Scarcity, Sneaking,<br>Forced Action, Obstruction, Misdirection | Text<br>**Dataset**: 53,000 product pages from around 11,000 shopping websites (GitHub - Aruneshmathur/Dark-Patterns: Code and Data Belonging to Our CSCW 2019 Paper: " Dark Patterns at Scale: Findings from a Crawl of 11K Shopping Websites" ., 2019). | Hierarchical Density-Based Spatial Clustering of Applications with Noise (HDBSCAN) | Only text-based dark patterns were taken, a few Selenium crashes were experienced, the crawler failed to complete the product purchase flow on some websites, crawled only product pages and checkout pages, and failed to capture dark patterns that appear after purchase. |

[1] https://www.domcop.com/top-10-million-websites

| S.No. | Research Articles | Types | Features | Techniques | Limitations |
|---|---|---|---|---|---|
| 7 | (Pedersen et al., 2023) | Trick Question, Sneak into Basket, Roach Model, Privacy Zuckering, Price Comparison, Prevention, Hidden Costs, Misdirection, Bait and Switch, Confirmshaming,<br>Disguised Ads, Forced Continuity, Friend Spam, Nagging, Obstruction, Sneaking,<br>Interface Interference,<br>Forced Action | Does not count, No choice, Multiple choice panels, Choice cascade, Widget inequality, Unlabeled sliders, Unmarked X, No antonyms.<br>**Dataset**: Screenshot of both the initial page of the Consent Management Platform (CMP) and the settings page of each visited site of Open Page Rank. | Optical Character Recognition (OCR) was utilised to retrieve the text from the screenshot.<br>Arrays of synonyms and antonyms were used to identify many of the dark patterns. | Div tags make it difficult to detect a CMP, only use three antonyms for each of the synonyms for accept and decline, and handle websites that do not actually offer a proper reject option on the CMP. Other CMP setups that Google uses do not have an option to reject and should be classified as a no-choice. |
| 8 | (Mansur SMH et al., 2023) | Sneaking, Urgency/Scarcity, Misdirection, Social Proof, Obstruction,<br>Forced Action, Nagging | Detecting icons, visuals, and text<br>**Dataset:** The ContextDP dataset contains 501 screenshots, which include 243 non-darkpattern (164 mobile and 79 web UI) screenshots and 301 screenshots containing dark patterns (GitHub - SageSELab/AidUI: This Repository Contains the Replication Package of Our ICSE' 23 Paper " AidUI: Toward Automated Recognition of Dark Patterns in User Interfaces," 2023) | AidUI framework: Detection technique: Region-based Convolutional Neural Networks (R-CNN), PyTorch, Torchvision, OCR, pattern matching (Spacy), or greyscale histogram (OpenCV) | AidUI is targeted toward 10 DP categories. Text analysis techniques are difficult to apply to certain DP categories (e.g., toying with emotion) that involve semantically complex textual patterns. |
| 9 | (Yada et al., 2023) | Sneaking, Urgency,<br>Scarcity, Misdirection,<br>Social Proof, Obstruction, Forced Action | Text<br>**Dataset:** Text-based dataset for e-commerce websites (Ec-Darkpattern/Dataset/Dataset.Tsv at Master · Yamanalab/Ec-Darkpattern · GitHub, 2022) | Trained a model using Bidirectional Encoder Representations from Transformers (BERT) and RoBERTa for automatic detection of dark patterns | The approximations are explained via post-hoc explanation techniques such as LIME and SHAP, which may not fully represent the internal reasoning of the model for complicated interactions. |
| 10 | (Gundelach & Herrmann D, 2023 | Obstruction, Interface Interference | Content of consent notices, Different colored buttons<br>**Dataset:** A random sample of the top 10,000 websites listed by Tranco manually annotated 1,000 websites for a ground-truth baseline. | Cookie scanner: detects and extracts consent notices using a BERT model for English notices, DOM tree walking, Perceptive detection, List-based Detection | Due to the changing nature of web content, decline option identification performed rather poorly.<br>Few websites denied access to the scanner by displaying a Cloudflare error message.<br>Scanner missed the notices located in shadow DOMs. |
| 11 | (Dmitry & Yerkebulan, 2022) | Trick questions, Sneak into basket, Roach Motel, Privacy Zuckering, Hidden Costs, Misdirection,<br>Price Comparison Prevention, Bait and Switch, Friend Spam, Confirmshaming, Disguised Ads, Forced Continuity | Complicated interface, Data leak, Cost increase, Impossibility to refuse, Hidden advertising<br>**Dataset:** 152 sites from various sources with dark patterns (GitHub - Aruneshmathur/Dark-Patterns: Code and Data Belonging to Our CSCW 2019 Paper: " Dark Patterns at Scale: Findings from a Crawl of 11K Shopping | Hierarchical and K-Means | Study is limited to Russian-language content and online services.<br>It uses linguistic variables and expert assessments from a small sample of respondents (20 students), which introduces bias and restrict the results. |

| S.No. | Research Articles | Types | Features | Techniques | Limitations |
|---|---|---|---|---|---|
| 12 | (Yada et al., 2022) | Sneaking, Obstruction, Forced Action, Nagging, Interface Inference | Text<br>**Dataset:** Text-based dataset (where dark pattern texts were obtained from (Ec-Darkpattern/Dataset/Dataset.Tsv at Master · Yamanalab/Ec-Darkpattern · GitHub, 2022) | Natural Language Processing (NLP) Methods (Bag-of-Words and Classical Machine Learning Model)<br>Transformer-based pre-trained language models (e.g., BERT) | Dark pattern texts are majorly from shopping websites which might not fully capture the range of dark patterns available.<br>The negative samples were also taken from the same websites as the dark patterns which introduce bias. |
| 13 | (Bajaj et al., 2025) | Pop-Ups or Overlays, Hidden Elements, Misleading Labels or Buttons, Pre-Selected Checkboxes, Misdirection, Obstruction, Fake Scarcity, Fake Social Proof, Fake Urgency | Text and Image<br>**Dataset:** 1 (Image dataset): 490 self-annotated images, providing a comprehensive collection of various web pages having dark patterns.<br>Dataset 2 (Dark Patterns text dataset) (Ec-Darkpattern/Dataset/Dataset.Tsv at Master · Yamanalab/Ec-Darkpattern · | Document Object Model (DOM) inspector to detect structure-based dark patterns, You Only Look Once version-5 (YOLOv5) for visual analysis, DistilBert and easyOCR for<br>text-based dark patterns. | Not suitable for identifying Pre-Selected Checkboxes,<br>Under more exacting matching constraints, the accuracy of YOLOv5 drastically declines. |
| 14 | (Schlolaut et al., 2024) | Address Book Leeching, Social Pyramid Schemes, Attention Grabber, Bad Defaults, Default Settings and Preselection, Bait and switch, Coercion, Confirmshaming, Disguised Ads, Scarcity, Distraction, Ease, Immortal Accounts, Interface Interference, Interruption, Social Proof, Misdirection, Obfuscation, Privacy Zuckering | Audio, Color, Fonts, Highlighting, Images, Mandatory field entries, Popup, Preselected checkboxes, Progress bar, Nested path, Wording | The idea is to use a crawler to examine websites in the context of deceptive patterns. Such a crawler could be a framework like Open Web Privacy Measurements (OpenWPM). | Only the types of deceptive patterns whose capture is technically feasible were considered. Hence, deceptive patterns that aim to trigger certain reactions in users through the content of images or texts were out of scope. |
| 15 | (Nouwens et al., 2020) | Interface Interference,<br>Obstruction, No Immediate Opt-Out | CMP’ s visual elements, interaction design, and textual content<br>**Dataset:** Top 10,000 most-visited websites in the United Kingdom. | Web scraper utilised the Python library Scrapy2 and JavaScript rendering service Splash3. | Unable to ensure that the dataset is free of false positives or false negatives, a 5–15 second wait included to allow the page to load before scraping might not always be sufficient, complexity of JavaScript Rendering. |
| 16 | (Ramteke et al., 2024) | Forced Action, Misdirection, Obstruction, Scarcity, Sneaking, Social Proof, Urgency, Not a Dark Pattern | Contextual sentence meaning<br>**Dataset:** Researched various e-commerce sites and publicly available datasets from platforms like Kaggle and GitHub were utilised. | Fine-tuned BERT’ s bidirectional sentence analysis language models, hyperparameter tuning, and generative capabilities | Struggle with visual elements containing text and interaction based. |

| S.No. | Research Articles | Types | Features | Techniques | Limitations |
|---|---|---|---|---|---|
| 17 | (Chen J et al., 2023) | Sneaking, Obstruction,<br>Forced Action, Nagging, Interface Inference, Misdirection, Hidden Information, Gamification, Drip Pricing | UI Element Property Extraction, like Color Extraction, UI Element Grouping, Icon Semantic Understanding, etc.<br>**Dataset:** Dataset contains 4,999 benign UIs and 1,353 malicious UIs of 1,660 instances spanning 1,023 mobile apps (Chen, 2023) | UIGuard: a knowledge-driven system that utilizes computer vision and natural language pattern matching | Some data types might be overlooked, or specific dark pattern samples might only show up a few times; the tool's performance on the newest user interfaces is not assured. |
| 18 | (Yue C et al., 2024) | Interface Interference, Sneaking | Textual content, UI elements<br>**Dataset:** 13,597 apps from Google Play and identified 589 subscription-based apps. | DarkFleece, a dark pattern-based Fleeceware Detector, which scrutinises the UI design of subscription-based apps to uncover dark patterns. | A well-labelled dataset for Fleeceware is limited. |
| 19 | (Kran et al., 2025) | Brand Bias, User Retention, Sycophancy, Anthropomorphisation, Harmful Generation, Sneaking | Large Language Models (LLM) prompts<br>**Dataset:** 660 text-based prompts[1] | DarkBench benchmark | Do not claim full coverage of all the motivations facing an LLM developer,<br>chatbot products have private system prompts that affect the chatbot' s behavior, making it impossible to systematically test these, augmented with further functionality that might change the frequency of dark patterns |
| 20 | (Hadan et al., 2024) | Temporal Patterns, Monetary Patterns, Social Patterns, Psychological Patterns | Psychological impact, Monetization goals, and Deceptive nature<br>**Dataset:** Recorded a 30-minute video. Multiple screenshots of each game mechanic were taken from the video (Game UI Database - Overwatch, 2024). | Game Mechanics Analysis | Potential Bias, Only Reddit-based data used led to incomplete coverage, Limited Time Frame, Specific to OW2 Findings |
| 21 | (Kocyigit et al., 2025) | False Hierarchy, Disguised Ads, Sneak into Basket, Hidden Costs, High Demand, Low Stock, Endorsement and Testimonials, Bad Defaults, Countdown Timer, Limited Time Message, Confirmshaming, Trick Questions, Activity Messages | Textual data, Visual Features<br>**Dataset:** Screenshots of DPs in web or mobile UIs<br>(GitHub - Kocyigitemre/Deceptilens: This Is a Repo of Ongoing Project., 2025) | DeceptiLens, a pre-trained MM-LLM (GPT-4o) based approach, empowered with the Chain-of-Thought (CoT) technique, and Retrieval Augmented Generation (RAG) framework | Additional information like HTML of webpage or user journey were not included. Only one recent ontology was considered, dataset was limited, and not all DP experts were included. |

[1] https://huggingface.co/datasets/anonymous152311/darkbench

- **Data Extraction and Processing:** Multiple methodologies have been employed to extract data from websites and applications, encompassing both textual and non-textual elements. These approaches include the extraction of textual content, UI components, and text from images and screenshots, as well as the analysis of behavioral tracking data, crowdsourced information, and user feedback. For textual data extraction, a range of tools and techniques have been utilized. These include Selenium WebDriver (Mathur et al., 2019; Ramteke et al., 2024), OpenWPM (Mathur et al., 2019; Schlolaut et al., 2024), the JavaScript library Puppeteer (Sazid & ENASE, 2024) and OCR technologies (Bajaj et al., 2025; Chen J et al., 2023; Mansur SMH et al., 2023; Pedersen et al., 2023). Additional methods involve pattern matching using SpaCy (Mansur SMH et al., 2023), the Python-based Scrapy framework, JavaScript rendering services such as Splash (Nouwens et al., 2020), and HTML parsing libraries like BeautifulSoup (Ramteke et al., 2024) .Document Object Model Inspector (DOMi) is used to extract content from HTML and XML-based files, while OCR is applied to retrieve information from screenshots and images (Pedersen et al., 2023) .Selenium also facilitates the downloading of homepage content from non-English websites, with the Polyglot Python library used for language detection (Mathur et al., 2019).

For non-textual data extraction, advanced tools such as Faster R-CNN(Ramteke et al., 2024), (Kocyigit et al., 2023), PyTorch (Mansur SMH et al., 2023), Torchvision (Mansur SMH et al., 2023), YOLOv5 (Bajaj et al., 2025; Yada et al., 2022) , OpenCV (Mansur SMH et al., 2023), and OCR are employed. For user feedback-based data, user complaints (Traubinger et al., 2024), Nielsen's 10 heuristic principles label classification (Dmitry & Yerkebulan, 2022), and LLM prompt-based approaches (Kran et al., 2025) were used. Behavioral tracking methods include event tracking (e.g., forced scrolls and automatic opt-ins) and cookie consent scanning tools (Gundelach & Herrmann D, 2023) enabling the identification of manipulative user experience strategies.

- **Classification and Detection:** Broadly, researchers commonly employ three primary approaches for the classification and detection of dark patterns. In addition to these, some studies have developed custom frameworks or integrated supplementary methods alongside their core approaches.
- **Bidirectional Encoder Representations from Transformers (BERT) Based Models:** A significant number of researchers have adopted BERT (Gundelach & Herrmann D, 2023) and its various derivatives for the classification and detection of dark patterns. One commonly used variant is a fine-tuned BERT model that leverages BERT's bidirectional sentence understanding and generative capabilities (Nouwens et al., 2020), DistilBERT, a streamlined and faster version of BERT, offers a 40% reduction in model size, operates 60% faster, and retains approximately 97% of BERT's language comprehension performance (Bajaj et al., 2025). Additional variants include pre-trained BERT (Yada et al., 2022), GPT-3 (Sazid & ENASE, 2024) trained BERT models and RoBERTa (Sazid & ENASE, 2024; Yada et al., 2023).
- **Clustering Techniques:** Clustering is another widely used method, aimed at grouping dark patterns based on shared characteristics. Common clustering techniques include K-Means and Hierarchical Clustering (Dmitry & Yerkebulan, 2022), as well as HDBSCAN (Mathur et al., 2019).
- **Custom Analytical Approaches:** Researchers have also developed several specialized analytical frameworks. These include the Layered Analysis of Persuasive Designs (Ahuja & Kumar, 2024), User Complaint Analysis (Traubinger et al., 2024), User Action Analysis (Nouwens et al., 2020), LLM-assisted K-shot Generation (Kran et al., 2025)and the AidUI Framework (Mansur SMH et al., 2023), which combines R-CNN with neural networks. Another notable method is Baseline Detection, which utilizes NLP techniques and transformer-based pre-trained language models (Yada et al., 2022).
- **Supporting Tools and Techniques:** To enhance these detection methods, researchers have employed additional tools such as UML activity diagrams (Kocyigit et al., 2023), web scrapers (Hildebrand & Nyquist, 2021), arrays of synonyms and antonyms (Pedersen et al., 2023), DOM tree walking, perceptive detection, and list-based detection (Gundelach & Herrmann D, 2023) as well as tools like UIGuard (Chen J et al., 2023).

### Evaluation

To assess the performance of various models, researchers have employed several evaluation metrics, with accuracy being a primary indicator of whether a model successfully identifies dark patterns.

Table 3 presents a comparison of the accuracy levels achieved by different techniques, including variants of the BERT model and custom frameworks.

**UIGuard** (Chen J et al., 2023), a knowledge-driven, rule-based system that relies solely on explicitly defined keywords, demonstrated the lowest accuracy among all evaluated methods. Its inability to interpret sentence semantics limits its detection capability to exact keyword matches, resulting in poor performance.

**DarkFleece** (Yue C et al., 2024) is built on 19 predefined features and lacks the flexibility to detect dark patterns beyond these constraints. It often fails to capture subtle or hidden manipulative cues, which also contributes to its relatively low accuracy.

**BERT** (Gundelach & Herrmann D, 2023; Ramteke et al., 2024; Yada et al., 2023), known for its bidirectional semantic understanding, serves as a foundational model for dark pattern detection due to its strong contextual language capabilities.

**DistilBERT** (Bajaj et al., 2025) ,a compressed version of BERT designed for speed and efficiency, exhibits slightly reduced accuracy compared to standard BERT, as it sacrifices some language comprehension during compression.

**ALBERT (A Lite BERT)** utilizes cross-layer parameter sharing and factorized embedding parameterization, which reduces its learning capacity and results in lower accuracy than the original BERT model (Yada et al., 2023)

**RoBERTa**, an enhanced version of BERT trained on a larger corpus, demonstrates a superior understanding of language and context. It consistently outperforms other models, with the RoBERTa-large variant achieving the highest reported accuracies—96.9% (Yada et al., 2023) and 97.5% (Yada et al., 2022). In contrast, UIGuard recorded the lowest accuracy of 93% (Chen J et al., 2023).

**Table 3: Accuracy of Techniques**

| | Techniques | Accuracy [In References] |
|---|---|---|
| **Deep Learning Techniques** | Fine-tuned BERT | 96% (Ramteke et al., 2024) |
| | DistilBERT | 95% (Bajaj et al., 2025) |
| | BERT base | 95.8% (Yada et al., 2023) 97.2% (Yada et al., 2022) |
| | BERT large | 96.7% (Yada et al., 2023) 96.5% (Yada et al., 2022) |
| | RoBERTa base | 96.5% (Yada et al., 2023) 96.6% (Yada et al., 2022) |
| | **RoBERTa large** | **96.9%** (Yada et al., 2023) **97.5%** (Yada et al., 2022) |
| | ALBERT base | 95.9% (Yada et al., 2022) |
| | ALBERT large | 96.5% (Yada et al., 2022) |
| | XLNet base | 96.6% (Yada et al., 2022) |
| | XLNet large | 94.2% (Yada et al., 2022) |
| **Custom Frameworks** | UIGuard | 93% (Chen J et al., 2023) |
| | DarkFleece | 93.43% (Yue C et al., 2024) |
| | DeceptiLens | 90.54% (Kocyigit et al., 2025) |

### Datasets

A wide range of datasets, including text, images and videos have been developed in effort to identify dark patterns each having its own merits and demerits. Text-based datasets like (Anonymous152311/Darkbench Datasets at Hugging Face, 2025; GitHub - Aruneshmathur/Dark-Patterns: Code and Data Belonging to Our CSCW 2019 Paper: "Dark Patterns at Scale: Findings from a Crawl of 11K Shopping Websites"., 2019) comprises of labeled examples of manipulative language, including compulsion, urgency, and confirm shaming. Their scalability and clarity make them perfect for training natural language processing (NLP) models, but they frequently lack interface context, which makes it difficult to spot structural or visual trickery. The visual manifestation of dark patterns through layout, color contrast, or deceptive buttons is captured by image-based datasets such as (GitHub - SageSELab/AidUI: This Repository Contains the Replication Package of Our ICSE'23 Paper "AidUI: Toward Automated Recognition of Dark Patterns in User Interfaces," 2023). Although their static nature may cause them to miss dynamic or interactive modifications, these are useful for computer vision tasks and UI analysis. Dynamic UI or video datasets like (Game UI Database - Overwatch, 2024) comprises of screenshots, videos and UI elements from gaming interfaces, thus serving as a crucial database of detecting dark patterns in games. However, these datasets are more difficult to annotate and handle at scale. Together these datasets highlight the growing need for comprehensive, multimodal datasets that combine text, visual layout, and temporal interaction data, with consistent annotations.

## Discussion

E-commerce websites have emerged as one of the most prominent domains for the widespread deployment of dark patterns, aligning with the findings of previous research (Mathur et al., 2019). The most prominent dark pattern types include Sneaking, Forced Action, Obstruction, and Misdirection (Please refer to section 3). These patterns have been associated with financial losses, psychological manipulation, and breach of user consent. Despite the adverse consequences for users, such deceptive practices continue to be deliberately employed by e-commerce platforms to maximize profits (Bajaj et al., 2025). This ongoing exploitation underscores the importance of increasing public awareness about dark patterns and their impact.

Past studies have expanded their focus beyond websites, identifying dark patterns across mobile applications, cookie consent banners, and other digital interfaces. A variety of ML and DL techniques have been adopted to detect these patterns, as illustrated in Figure 3. Among the ML approaches, HDBSCAN (Mathur et al., 2019) K-Means, and Hierarchical Clustering (Dmitry & Yerkebulan, 2022) along with web scraping tools (Hildebrand & Nyquist, 2021) have been widely used. However, these techniques face notable limitations, including overfitting, difficulty detecting dynamic UI elements, and inadequate handling of non-textual content (Chu, 2025).

To overcome these challenges, many researchers have increasingly turned to advanced DL models. These include BERT (Gundelach & Herrmann D, 2023; Ramteke et al., 2024; Yada et al., 2022, 2023), DistilBERT (Bajaj et al., 2025), RoBERTa (Sazid & ENASE, 2024; Yada et al., 2023), GPT-3 (Sazid & ENASE, 2024), R-CNN (Mansur SMH et al., 2023), and other transformer-based or LLM-assisted models (Kran et al., 2025). In parallel, several customized frameworks have been developed, such as Complaint/User Action Analysis (Traubinger et al., 2024), the AidUI Framework (Mansur SMH et al., 2023), UIGuard (Chen J et al., 2023), and Baseline Detection Approaches (Yada et al., 2022). These frameworks are often enhanced with complementary techniques such as DOM tree traversal (Gundelach & Herrmann D, 2023), web scraping (Hildebrand & Nyquist, 2021), and UML-based modelling (Kocyigit et al., 2023). Among these, BERT has emerged as a foundational model for numerous detection strategies.

Regarding datasets, the dark pattern dataset created by (Mathur et al., 2019) based on a large-scale crawl of over 11,000 e-commerce websites (GitHub - Aruneshmathur/Dark-Patterns: Code and Data Belonging to Our CSCW 2019 Paper: “Dark Patterns at Scale: Findings from a Crawl of 11K Shopping Websites”., 2019) has been instrumental in advancing empirical research. Although multiple datasets exist, most are limited in scope, often focusing on a single domain such as e-commerce or gaming. Consequently, there is a growing demand for comprehensive, cross-platform datasets that can capture the diverse range of UI components and design patterns used in digital environments.

Despite considerable progress in detection techniques, no existing model is capable of identifying all types of dark patterns across all digital platforms. Critical gaps remain, particularly in detecting deceptive design patterns in chatbots, XR, and AR applications, especially in immersive gaming contexts, which remain largely underexplored.

As UI design continues to evolve, developers have adopted increasingly sophisticated and dynamic design elements, often embedding emotionally manipulative visual cues such as “Only 1 left in stock,” “I hate to save money,” and “No thanks, I don't need offers.” Our analysis reveals that dark patterns manifest in multiple formats, including text, images, video, cookies, advertisements, hyperlinks, and interactive design elements spanning a wide range of platforms.

This growing complexity signals the need for a unified detection framework that can systematically identify dark patterns in their various forms and contexts. Such a framework would enhance user protection and promote ethical design practices. Collaboration between developers, regulators, and researchers is essential in advancing this effort.

From a policy perspective, several jurisdictions have begun addressing dark patterns through legislative and regulatory action. In the United States, the California Privacy Rights Act (CPRA, 2023), an amendment to the California Consumer Privacy Act (CCPA) and the Colorado Privacy Act (CPA, 2023), provides a legislative foundation for dark pattern regulation (Nousiainen & Ortega, 2023). The Federal Trade Commission (FTC) has also invoked Section 5 of the FTC Act to address unfair and deceptive practices. A landmark case involved a $520 million fine levied against Epic Games for deploying dark patterns in Fortnite, marking the most significant penalty of its kind (King & Stephan, 2021; Nousiainen & Ortega, 2023).

In India, the Central Consumer Protection Authority (CCPA) has issued an advisory directing e-commerce platforms to conduct self-audits within three months of receiving the notice to eliminate dark patterns from their platforms. Additionally, the Department of Consumer Affairs released the 2023 Guidelines for Prevention and Regulation of Dark Patterns, which outline 13 identified deceptive practices. These include False Urgency, Basket Sneaking, Confirm shaming, Forced Action, Subscription Traps, Interface Interference, Bait and Switch, Drip Pricing, Disguised Ads, Nagging, Trick Wording, SaaS Billing, and Rogue Malwares (Press Release: Press Information Bureau, 2025). However, no single law currently addresses the full spectrum of dark patterns in use today (King & Stephan, 2021).

Therefore, more robust research, enhanced government support, and public education are essential to effectively combat dark patterns. Many users remain unaware of the deceptive mechanisms influencing their behavior. Empowering them with awareness and access to detection tools is a crucial step toward creating transparent, ethical, and user-centric digital ecosystems.

## Conclusion

This study presents a systematic review of dark pattern detection and analysis across a broad spectrum of digital platforms, including mobile applications, websites, cookies, chatbots, and XR/AR-based interfaces. The findings demonstrate that dark patterns can manifest in various formats, such as text, images, videos, and hyperlinks and are commonly organised into structured taxonomies based on their functional characteristics. A considerable number of studies leverage Mathur's dataset as a benchmark for training and evaluating ML models for dark pattern detection. Among the various detection models, BERT is widely used as a foundational architecture; however, RoBERTa consistently outperforms it in terms of detection accuracy. This review does not restrict itself to a specific interface type or geographic regions, thereby offering a holistic overview of current research efforts. The insights gained from this analysis would be helpful in guiding future advancements in developing user-centric, ethically designed digital environments, fostering greater awareness and mitigating dark patterns in digital design.

## References

1. Ahuja, S., & kumar J. (2022). Conceptualizations of user autonomy within the normative evaluation of dark patterns. Springer Ethics and Information Technology, 2022., 24(4). https://doi.org/10.1007/S10676-022-09672-9
2. Ahuja, S., & Kumar, J. (2024). Layered Analysis of Persuasive Designs: A Framework for Identification and Autonomy Evaluation of Dark Patterns. Mobilizing Research and Regulatory Action on Dark Patterns and Deceptive Design Practices Workshop at CHI Conference on Human Factors in Computing Systems, May 12, 2024, Honolulu, HI (Hybrid Workshop). https://ceur-ws.org/Vol-3720/paper1.pdf
3. Bajaj, A., Uppal, K., Razdan, R., Tuteja, Y., Bhardwaj, A., & Abraham, A. (2025). A Comprehensive Analysis for Dark Pattern Detection Using Structural, Visual and Textual Information. International Journal of Computer Information Systems and Industrial, 2025. Cspub-Ijcisim.Org, 17, 14–25. https://cspub-ijcisim.org/index.php/ijcisim/article/view/1013
4. Bösch, C., Erb, B., Kargl, F., Kopp, H., & Pfattheicher, S. (2016). Tales from the dark side: Privacy dark strategies and privacy dark patterns. Proceedings on Privacy Enhancing Technologies, 2016, 2016(4), 237–254. https://doi.org/10.1515/popets-2016-0038
5. Brignull, H., Leiser, M., Santos, C., & Doshi, K. (2023). Deceptive patterns – user interfaces designed to trick you. deceptive.design. https://www.deceptive.design/types
6. Chen, J. (2023). Datasets and Detection Rules for UIGuard. https://doi.org/10.5281/ZENODO.8126443
7. Chen J, Xing Z, Lu Q, Sun J, Feng S, Xu X, & Chen C. (2023). Unveiling the tricks: Automated detection of dark patterns in mobile applications. Proceedings of the 36th Annual ACM Symposium on User Interface Software and Technology. https://doi.org/10.1145/3586183.3606783
8. Chu, D. (2025). Into the Dark The Fault of Machine Learning Methods in Detecting UX Dark Patterns. https://aaltodoc.aalto.fi

9. Conti, G., & Sobiesk E. (2010). Malicious interface design: exploiting the user. Proceedings of the 19th International Conference on World Wide Web, 271–280. https://doi.org/10.1145/1772690.1772719

10. Dmitry, N., & Yerkebulan, B. (2022). Clustering of Dark Patterns in the User Interfaces of Websites and Online Trading Portals (E-Commerce). Mathematics, 10(18). https://doi.org/10.3390/math10183219

11. GitHub - ec-darkpattern/dataset/dataset.tsv at master · yamanalab/ec-darkpattern ·(2022). https://github.com/yamanalab/ec-darkpattern/blob/master/dataset/dataset.tsv

12. FTC. (2024, July 10). FTC, ICPEN, GPEN Announce Results of Review of Use of Dark Patterns Affecting Subscription Services, Privacy _ Federal Trade Commission. Federal Trade Commission. https://www.ftc.gov/news-events/news/press-releases/2024/07/ftc-icpen-gpen-announce-results-review-use-dark-patterns-affecting-subscription-services-privacy

13. Game UI Database - Overwatch. (2024). https://www.gameuidatabase.com/gameData.php?id=1341

14. GitHub - aruneshmathur/dark-patterns: Code and data belonging to our CSCW 2019 paper: “Dark Patterns at Scale: Findings from a Crawl of 11K Shopping Websites”. (2019). https://github.com/aruneshmathur/dark-patterns

15. GitHub - kocyigitemre/deceptilens: This is a repo of ongoing project. (2025). https://github.com/kocyigitemre/deceptilens

16. GitHub - SageSELab/AidUI: This repository contains the replication package of our ICSE’23 paper “AidUI: Toward Automated Recognition of Dark Patterns in User Interfaces.” (2023). https://github.com/SageSELab/AidUI

17. GitHub - vertr/ChIPS-dataset. (2024). https://github.com/vertr/ChIPS-dataset

18. GitHub - yasin-sazid/dark-patterns-bangladesh. (2024). https://github.com/yasin-sazid/dark-patterns-bangladesh

19. Gray, C. M., Mildner, T., & Gairola, R. (2025, April 26). Getting Trapped in Amazon’s “Iliad Flow”: A Foundation for the Temporal Analysis of Dark Patterns. Conference on Human Factors in Computing Systems - Proceedings. https://doi.org/10.1145/3706598.3713828

20. Gray, C. M., Santos, C. T., Bielova N, & Mildner, T. (2023). An Ontology of Dark Patterns: Foundations, Definitions, and a Structure for Transdisciplinary Action. Proceedings of the 2024 CHI Conference on Human Factors in Computing Systems At Honolulu, Hawai’i. https://doi.org/10.1145/3613904.3642436

21. Gundelach, R., & Herrmann D. (2023). Cookiescanner: An automated tool for detecting and evaluating gdpr consent notices on websites. Proceedings of the 18th International Conference on Availability. https://doi.org/10.1145/3600160.3605000

22. Hadan, H., Zhang-kennedy, L., Nacke, L. E., & Alicia Sgandurra, S. (2024). From Motivating to Manipulative: The Use of Deceptive Design in a Game’s Free-to-Play Transition. Proceedings of the ACM on Human-Computer Interaction, 8(CHI PLAY), 1–31. https://doi.org/10.1145/3677074

23. Hildebrand, T. L., & Nyquist, F. (2021). Cookies, GDPR and Dark patterns: Effect on consumer privacy. Blekinge Institute of Technology, 371 79 Karlskrona, Sweden. https://www.diva-portal.org/smash/record.jsf?pid=diva2:1570073

24. King, J., & Stephan, A. (2021). REGULATING PRIVACY DARK PATTERNS IN PRACTICE-DRAWING INSPIRATION FROM CALIFORNIA PRIVACY RIGHTS ACT. GEORGETOWN LAW TECHNOLOGY REVIEW. https://perma.cc/WYG9-Z4H5].

25. Kocyigit, E., Rossi, A., & Lenzini, G. (2023). Towards assessing features of dark patterns in cookie consent processes. FIP International Summer School on Privacy and Identity Management, 671 IFIP, 165–183. https://doi.org/10.1007/978-3-031-31971-6_13

26. Kocyigit, E., Rossi, A., Sergeeva, A., Negri Ribalta, C., Farjami, A., & Lenzini, G. (2025). DeceptiLens: an Approach supporting Transparency in Deceptive Pattern Detection based on a Multimodal Large Language Model. Association for Computing Machinery (ACM), 1942–1959. https://doi.org/10.1145/3715275.3732129

27. Kran, E., Nguyen, J., Kundu, A., Jawhar, S., Park, J., & Jurewicz, M. (2025). DarkBench: Benchmarking Dark Patterns in Large Language Models. OpenrevieThe Thirteenth International Conference on Learning Representations. https://openreview.net/forum?id=odjMSBSWRt

28. Krauß, V., Saeghe, P., Boden, A., Khamis, M., McGill, M., Gugenheimer, J., & Nebeling, M. (2024). What Makes XR Dark? Examining Emerging Dark Patterns in Augmented and Virtual Reality through Expert Co-Design. ACM Transactions on Computer-Human Interaction, 31(3). https://doi.org/10.1145/3660340

29. Lewis, F. B. W., & Vassileva, J. (2024). Integrating Dark Pattern Taxonomies. ArXiv:2402.16760 [Cs.CY]. https://arxiv.org/pdf/2402.16760

30. Mansur SMH, Salma S, Awofisayo D, & Moran K. (2023). Aidui: Toward automated recognition of dark patterns in user interfaces. IEEE/ACM 45th International Conference on Software Engineering (ICSE) (Pp. 1958-1970). IEEE. https://ieeexplore.ieee.org/abstract/document/10172754/

31. Mathur, A., Acar, G., Friedman, M. J., Lucherini, E., Mayer, J., Chetty, M., & Narayanan, A. (2019). Dark patterns at scale: Findings from a crawl of 11K shopping websites. Proceedings of the ACM on Human-Computer Interaction, 2019. Dl.Acm.Org, 3(CSCW), 32. https://doi.org/10.1145/3359183

32. Mathur, A., Kshirsagar, M., & Mayer, J. (2021). What makes a dark pattern... dark? Design attributes, normative considerations, and measurement methods. Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems, 2021. Dl.Acm.Org. https://doi.org/10.1145/3411764.3445610

33. Meinhardt, L.-M., Demharter, S., Rietzler, M., Colley, M., Eßmeyer, T., & Rukzio, E. (2025). Mind Games! Exploring the Impact of Dark Patterns in Mixed Reality Scenarios. ArXiv Preprint ArXiv:2506.06774. https://doi.org/10.1145/3743709

34. Mukherjee, C., Mohamed, R., Arunasalam, A., Farrukh, H., & Berkay Celik, Z. (2025). Shadowed Realities: An Investigation of UI Attacks in WebXR.

35. Nousiainen, K., & Ortega, C. P. (2023). Dark Patterns in Law and Economics Framework Dark Patterns in Law and Economics Framework DARK PATTERNS IN LAW AND ECONOMICS FRAMEWORK. Loyola Consumer Law Review, 36(1). https://doi.org/10.1787/44f5e846

36. Nouwens, M., Liccardi, I., Veale, M., Karger, D., & Kagal, L. (2020). Dark patterns after the GDPR: Scraping consent pop-ups and demonstrating their influence. Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems. https://doi.org/10.1145/3313831.3376321

37. Page, M. J., McKenzie, J. E., Bossuyt, P. M., Boutron, I., Hoffmann, T. C., Mulrow, C. D., Shamseer, L., Tetzlaff, J. M., Akl, E. A., Brennan, S. E., Chou, R., Glanville, J., Grimshaw, J. M., Hróbjartsson, A., Lalu, M. M., Li, T., Loder, E. W., Mayo-Wilson, E., McDonald, S., … Moher, D. (2021). The PRISMA 2020 statement: An updated guideline for reporting systematic reviews. The BMJ, 372. https://doi.org/10.1136/BMJ.N71

38. Pedersen, M., Guribye, F., & Slavkovik M. (2023). Automatic detection of manipulative Consent Management Platforms and the journey into the patterns of darkness. Proceedings of the 5th Symposium of the Norwegian AI Society. https://bora.uib.no/bora-xmlui/handle/11250/3088667

39. Potel-Saville, M., & Da Rocha, M. (2024). From Dark Patterns to Fair Patterns? Usable Taxonomy to Contribute Solving the Issue with Countermeasures. In Annual Privacy Forum (Pp. 145-165). Cham: Springer Nature Switzerland., 13888 LNCS, 145–165. https://doi.org/10.1007/978-3-031-61089-9_7

40. Press Release:Press Information Bureau. (2025). https://www.pib.gov.in/PressReleasePage.aspx?PRID=2134765

41. Ramteke, A., Tembhurne, S., Sonawane, G., & Bhimanpallewar, R. N. (2024). Detecting Deceptive Dark Patterns in E-commerce Platforms. ArXiv Preprint ArXiv:2406.01608. https://arxiv.org/pdf/2406.01608

42. Sazid, Y., & ENASE, K. S. (2024). Prevalence and User Perception of Dark Patterns: A Case Study on E-Commerce Websites of Bangladesh. In Proceedings of the 19th International Conference on Evaluation OfNovel Approaches to Software Engineering (ENASE 2024), 238–249. https://doi.org/10.5220/0012734900003687

43. Schlolaut, M., Kieselmann, O., & Wacker, A. (2024). Comparing Nudges and Deceptive Patterns at a Technical Level. Workshop at CHI Conference on Human Factors in Computing Systems, May 12, 2024, Honolulu, HI(HybridWorkshop). https://athene-forschung.unibw.de/doc/150142/150142.pdf

44. Traubinger, V., Heil, S., Grigera, J., Garrido, A., & Gaedke, M. (2024). In Search of Dark Patterns in Chatbots. International Workshop on Chatbot Research and Design, 2023, 14524 LNCS, 117–132. https://doi.org/10.1007/978-3-031-54975-5_7

45. Yada, Y., Feng, J., Matsumoto, T., Fukushima, N., Kido, F., & Yamana, H. (2022). Dark patterns in e-commerce: a dataset and its baseline evaluations. IEEE International Conference on Big Data (Big Data). https://ieeexplore.ieee.org/abstract/document/10020800/

46. Yada, Y., Matsumoto, T., Kido F, & Yamana H. (2023). Why is the User Interface a Dark Pattern?: Explainable Auto-Detection and its Analysis. IEEE International Conference on Big Data (BigData), 2023. https://ieeexplore.ieee.org/abstract/document/10386308/

47. Yue C, Zhong C, Chen K, Zhang Z, & Lee Y. (2024). {DARKFLEECE}: Probing the Dark Side of Android Subscription Apps. In 33rd USENIX Security Symposium (USENIX Security 24) (Pp. 1543-1560). https://www.usenix.org/conference/usenixsecurity24/presentation/yue.