DEIM Forum 2022 E21-4

ショッピングサイトを対象としたダークパターン自動検出の試み

矢田　宙生† 　馮　 佳櫻†† 　松本　恒雄†††,†††† 　福島　直央††††† 　木戸　冬子††††††,†††

山名　早人†††††††

† 早稲田大学基幹理工学部　〒 169–8555 東京都新宿区大久保 3-4-1
††††††† 早稲田大学理工学術院　〒 169–8555 東京都新宿区大久保 3-4-1
†† 早稲田大学院基幹理工学研究科　〒 169–8555 東京都新宿区大久保 3-4-1
††† 早稲田大学理工学術院総合研究所　〒 169–8555 東京都新宿区大久保 3-4-1
†††† 国民生活センター　〒 252-0229 神奈川県相模原市中央区弥栄 3-1-1
††††††† 国立情報学研究所　〒 101-8430 東京都千代田区一ツ橋 2-1-2
††††† LINE 株式会社 公共戦略室　〒 160–0004 東京都新宿区四谷 1-6-1
E-mail: †{yadayuki,kayouh,yamana}@yama.info.waseda.ac.jp, ††{tsuneo.matsumoto,fkido}@aoni.waseda.jp,
†††nao.fukushima@linecorp.com

あらまし　ダークパターンとは，ユーザ自身が意図しない行動を取るよう巧妙に設計されたユーザインターフェースであり，近年問題視されている. 従来，Web 上でのダークパターン大規模調査やダークパターンの人手による分類などが行われてきている. しかし，ユーザを守るためには，こうしたダークパターンを自動的に検出し，ユーザに注意を促すことが必要となる. そこで，本稿では，ショッピングサイトを対象に，様々な機械学習手法を用いてダークパターンの自動検出実験を行った. 実験においては，Mathur 氏らが 2019 年に公開したダークパターンのテキストを正例とした．負例としては，同テキストが掲載されているサイトから収集したダークパターン以外のテキストを用いた．機械学習手法として，SVM，勾配ブースティング，BERT を適用した. 結果，BERT による自動検出モデルにおいて，F 値 0.962 を得た.

キーワード　ダークパターン，ショッピングサイト，BERT，GBDT，SVM

1 はじめに

ダークパターンは，ユーザ自身が意図しない行動を取るよう巧妙に設計されたユーザインターフェースである．ダークパターンは多くの Web サイトやアプリケーションに存在することが分かっており，近年問題視されている [5,12,13]．ユーザをダークパターンから保護するためには，ダークパターンを自動的に検出し，ユーザに存在を周知する必要がある．本論文では，先行研究 [1] により，様々な種類のダークパターンが多く存在することが確認されているショッピングサイトを対象に，[1] において収集されたダークパターンのテキストを正例とし，ダークパターンの自動検出の実験を行う．これにより，現状の技術での検出率を明らかにする．

ダークパターンは，2010 年 Harry [4] によって，「ユーザ自身が意図しない行動を取るように巧妙に設計されたユーザインターフェース」と定義された．以後，様々な研究を通してダークパターンに関する調査が行われている．ショッピングサイトやクッキーへの同意，人気の高いアプリケーション等を対象に大規模調査が行われており，インターネットサービス上の至る所にダークパターンが存在していることがわかっている．しかし，インターネットサービス上のダークパターンからユーザを保護するための具体的な解決策は提案されていない.

本稿では，インターネットサービス上のダークパターンからユーザを保護することを目的に，ダークパターンの自動検出に関する実験・評価を行う．具体的には，Mathur らが収集したショッピングサイトにおけるダークパターンのテキストデータ [1] とスクレイピングにより収集したショッピングサイトにおけるダークパターンではないテキストデータを用いて，機械学習によるショッピングサイトにおけるダークパターンの自動検出に関する実験を行う．機械学習アルゴリズムには線形 SVM，LightGBM [8]，BERT [9] を使用する.

本論文の構成は以下の通りである．2 節では本論文の主要な背景知識であるダークパターンとダークパターンに関する議論について説明する． 3 節では本論文における関連研究を示す. 4 節で提案 手法の詳細を説明する．5 節で提案手法の性能を実験により評価する．最後に 6 節で結論を示す.

2 背景知識

2.1 ダークパターン

ダークパターンはユーザ自身が意図しない行動を取るよう巧妙に設計されたユーザインターフェースの総称である． ダークパターンは，2010 年 Harry [4] が公開した Web サイト上で

初めて紹介・定義された．その種類は多岐に渡り [2]，実際の Web サイトやアプリケーションを対象にした調査によって，インターネットサービス上の至る箇所に，様々なダークパターンが存在することがわかっている．

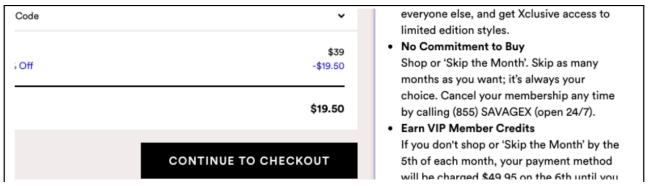

図 1　ダークパターンの実例 (savagex.com)

ダークパターンの具体的な事例を図 1 に示す．図 1 に示すダークパターンは Mathur ら [1] がショッピングサイトを対象に行ったダークパターンの大規模調査により得られた「Obstruction」という種類のダークパターンである．図 1 の例では”Cancel your membership any time by calling”と記載されているが，図に示される通り退会は電話に限定されている．つまり，有料会員登録はインターネット上からできるにも関わらず，退会を電話に限ることで退会を意図的に難しくしていると言える．「Obstruction」は例で示すように，契約の解除や退会といったインターネットサービスにとって不都合な操作を意図的にしづらくするようにデザインされたダークパターンである．

2.2　ダークパターンに関する議論

ダークパターンに関する議論は学術界のみではなく，様々な場所で行われている．

フランス共和国データ保護機関（CNIL）は, 2020 年に, ユーザインターフェースがデータ保護に与える影響について議論し，レポートを公表した [12]．デザインとユーザ行動の関係性やユーザのプライバシーに悪影響を与える可能性があるデザインやその具体例について議論をした．その中で, データ保護の観点でユーザに悪影響を与える可能性がある UI・ダークパターンを 4 つのカテゴリーに分類した (「PUSHING THE INDIVIDUAL TO ACCEPT SHARING MORE THAN WHAT IS STRICTLY NECESSARY」,「INFLUENCE　CONSENT」,「CREATING FRICTION ON DATA PROTECTION ACTIONS」,「DIVERTING THE INDIVIDUAL」).

カリフォルニア州は，2020 年に，消費者の，特にプライバシーに関連する選択に大きな影響を与えるようなインターネット上のダークパターン禁止することを消費者プライバシー保護法 (CCPA) の中で規定 [5] している．

OECD(経済開発協力機構) は，2020 年に，ダークパターンによって，消費者に生じるリスクや消費者をダークパターンから保護する法案を施行する際に生じる課題等に対する理解を深めることを目的とした会議を行った [13]．会議内では，ダークパターンの種類やそれらがユーザに与える影響に関する議論が行われた．

3　関 連 研 究

3.1　ダークパターンの種類に関する調査研究

ダークパターンの種類の定義自体を目的とした研究や大規模調査によって得られたダークパターンを独自に分類し，新たに種類を定義した研究等により，ダークパターンの種類は様々な定義がされている．

Colin ら [6] は，2018 年に，Google・Bing といった検索プラットホームや Facebook・instagram 等の SNS 上で，”dark patterns”やそれらに派生する言葉を検索することを通して，ダークパターンの事例を収集した．それらのコンテンツを分析し，ダークパターンを 5 種類に分類した．Colin らが定義した 5 種類のダークパターンを表 1 に示す．

表 1　Colin らが定義したダークパターンの種類 [6]

ダークパターンの種類	説明
Nagging	ユーザの操作の妨害や，特定の操作 (有料会員への登録等) への誘導を 目的として，特定の機能 (ポップアップ等) を複数回表示する．
Obstruction	退会や契約解除といった サービスにとって， 不都合な操作を意図的に難しくする．
Sneaking	ユーザに必要な情報を意図的に隠す．
Interface Interference	ユーザが特定の操作をするように誘導する．
Forced Action	ユーザが特定の操作をするように強制する．

「ダークパターン」という言葉を Web サイト上で初めて定義した Harry ら [4] は，2010 年に，ダークパターンを 12 種類に分類し，それぞれの種類のダークパターンに対する事例を紹介した．Harry らが定義した 12 種類のダークパターンを表 2 に示す．

以上のように，ダークパターンの種類は，複数の研究で定義されている．Mathur ら [2] は先行研究を通して定義されている様々な種類のダークパターンが，ユーザのサービス利用における意思決定をどの様にして誘導するかを調査した．調査対象としたのは 11 の学術的研究や法案等で定義されているの合計 85 種類のダークパターンである．

3.2　ダークパターンの大規模調査に関する研究

Mathur ら [1] は，2019 年に，ショッピングサイトを対象にダークパターンの大規模な調査を行った．調査対象としたのは，Alexa Traffic Rank(https://www.alexa.com/topsites) により取得したアクセス数の多い 361,102 件の Web サイトから英語のショッピングサイトのみを抽出することにより得られた 11,286 件のショッピングサイトである．その結果，約 11.1%である 1,254 件のショッピングサイトから，7 種類・1,818 件のダークパターンを発見し，そのテキストデータを公開した．

Di ら [7] は，2020 年に，240 の人気のある Android 用のアプリケーションを対象に調査を行った．二人の研究者によってユーザ登録や設定の変更といった一般的な動作を行い，アプリ

表 2　Harry らが定義したダークパターンの種類 [4]

ダークパターンの種類	説明
Trick questions	入力フォーム等でユーザが意図していない回答をするように誘導する質問を設置する.
Sneak into Basket	商品の購入プロセスの途中で, ユーザが選択していない追加商品を買い物カゴに忍ばせる.
Roach Motel	サブスクリプション等で登録や入会など契約を締結する作業は容易にできるようにしているが, 一方で契約の解約は容易にはできないようにデザインされている.
Privacy Zuckering	ユーザが入力した情報をサービスプロバイダが外部業者に許可なく売買し, ユーザの個人情報が漏洩する.
Price Comparison Prevention	他の商品の価格情報を隠すことにより, 価格の比較ができないようにデザインされている.
Misdirection	意図的にユーザの意識が特定の選択肢へと集中するようにデザインされている.
Hidden Costs	商品の購入においてユーザへの周知なしに追加費用が発生する.
Bait and Switch	機能 (メール配信等) の同意を求めるポップアップを拒否するつもりで閉じたら, 勝手に有効にされてしまうなど, 操作に対して, ユーザが意図していないような挙動を示す.
Confirmshaming	あるユーザの選択が当該ユーザにとって罪悪感を抱かせるようなものにしてある.
Disguised Ads	ユーザのクリックを促すために, ページ内のコンテンツであるかのようにデザインされた広告.
Forced Continuity	フリートライアルの終了後, 契約が自動更新され, 口座から金銭が引き落とされてしまう.
Friend Spam	ユーザがサービスに登録したメールアドレスから, 当該ユーザがそれまでにメールした他人のメールアドレスを対象に, サービスへの招待等の内容のスパムメールが許可なく送信されてしまう.

ケーション内にダークパターンが存在するか否かを調べた．調査の結果，全部で 1,787 のダークパターンが確認され，調査対象としたアプリケーションの 95%にダークパターンが存在することがわかった．Di らは発見されたダークパターンを分析し，Colin ら [6] が定義した 5 種類のダークパターンに分類した．

Soe ら [14] は，2020 年に，Cookie への同意通知に関するダークパターンの大規模調査を行った．調査対象は北欧語・英語で記述された 300 のニュースサイトにおける Cookie への同意通知である．二人の研究者によって,「同意通知内にダークパターンが存在するかどうか．存在する場合はその種類は何か．(Colin らが定義した 5 種類のダークパターン)」「Cookie への拒否をすることが可能かどうか」「Cookie への同意通知が表示される位置」といった点について手動で調査を行った．その結果，クッキーへの同意を誘発するためのダークパターン 297 件を確認した．

Mathur ら [3] は，2018 年に，インフルエンサーらがコンテンツ内で特定の商品を宣伝する際，そのコンテンツが広告である旨が開示されているか否かを大規模に調査した．アメリカの連邦取引委員会 (FTC) はクリエーターにユーザへの開示無しに，コンテンツ内で特定の商品等を宣伝することを禁止している．Mathur らは，500,000 の YouTube のコンテンツと 210,000 の Pinterest のコンテンツを調査した．その結果，アフィリエイト広告を含むコンテンツの約 10%のみしか，広告である旨の開示を行なっていないことが分かった．

3.3　ダークパターンがユーザに与える影響の調査研究

Kerstin ら [10] は，2021 年に，被験者実験を通して，ユーザが悪意を持ったデザインに気づくか否か，またどのような影響を受けるかを調査した．その結果，ダークパターンが調査対象のアプリケーション内に存在するということを事前に知らされた場合の方が，事前に知らされない場合に比較し，アプリケーション内に存在するダークパターンに気付きやすいことが分かった．

Thomas ら [15] は，2021 年に，Facebook を対象にダークパターンに関する調査を行った．2004 年から 2020 年までの Facebook の UI デザインをクローリングにより取得し，それらの UI デザインの変化を分析・比較することによって，ダークパターンが存在するか否かを調査した．調査の結果，colin らが定義したダークパターンの種類の一つである interface interference が確認された．また，Facebook を普段から使用している 116 人の人々に対して，Facebook を使用する意欲や満足度，プライバシーに関する懸念等に関するアンケートを行った．その結果，一部のユーザは SNS に対して懸念を示しており，精神的な問題についても指摘していることがわかった．

4　ダークパターンの自動検出実験

本節では，機械学習によってダークパターンの自動検出を行い，その適合率（精度）を確認する．具体的には，ショッピングサイトを対象に，ショッピングサイト中のテキストデータに対してダークパターンか否かを自動判定する．なお，本提案手法は，ショッピングサイト内にダークパターンが存在することを機械的に検出し，ユーザがダークパターンに騙されることを防ぐことを目的としている．

以下の構成で提案手法に関する説明を行う．4.1 節では提案手法の概要に関する説明を行う．4.2 節では自動検出器の学習に用いたデータセットに関する説明を行う．4.3 節では LightGBM，線形 SVM による自動検出器に関する説明を行う．4.4 節では

BERT による自動検出器に関する説明を行う．

4.1 自動検出器の概要

本提案手法の概要を述べる．本提案手法では，ショッピングサイトにおけるダークパターンに該当するテキストデータとショッピングサイトにおけるダークパターンに該当しないテキストデータを，機械学習モデルで学習することによって，ショッピングサイトにおけるダークパターンの自動検出器を作成する．機械学習モデルには，線形 SVM，LightGBM，BERT を用いた．

4.2 データセット

機械学習に用いるデータとして，Mathur らが Github 上で公開しているショッピングサイトを対象としたダークパターンのテキストデータ [1] [1] を正例として用いるとともに，負例として，ダークパターンではないテキストデータを収集した．最終的に，正例と負例が 1 対 9 の割合になるようデータを準備し，正例 1,178 件，負例 10,602 件のデータセットを構築した．

Mathur らは，ショッピングサイトを対象にダークパターンの大規模調査を行い，ショッピングサイトの約 11%，1,254 のショッピングサイトから，1,818 件のダークパターンと判定されたテキストを収集している．これらのダークパターンは，表 4 に示す 7 種類に分類される．これら 1,818 件のダークパターンテキストの内，欠損や重複しているテキストデータを除いた 1,178 件のテキストデータを正例として用いる．図 2 に，1,178 件のテキストデータのダークパターンの種類毎の分布を示す．また，表 3 に 1,178 件のテキストデータの単語数に関する統計量を示す．なお，全てのテキストデータは英語で記述されている

表 3　ダークパターンに該当するテキストの単語数に関する統計量

平均値	標準偏差	最小値	中央値	最大値
9.13	12.9	1	6	143

表 4　ダークパターンの種類 [1]

ダークパターンの種類	説明
Scarcity	商品の希少性を強調し，ユーザに購入を促す．
Social Proof	他のユーザが購入している などの情報で， ユーザに購入を促す．
Urgency	商品に対する緊急性を必要以上に強調する．
Misdirection	ユーザに，特定の選択肢を選択させるもしくは選択させないように誘導する．
Obstruction	ユーザが特定の行動を取ることをしづらくするようにする．
Sneaking	ユーザにとって必要な情報を隠す．
Forced Action	ユーザが特定の行動をするように強制する．

1：https://github.com/aruneshmathur/dark-patterns

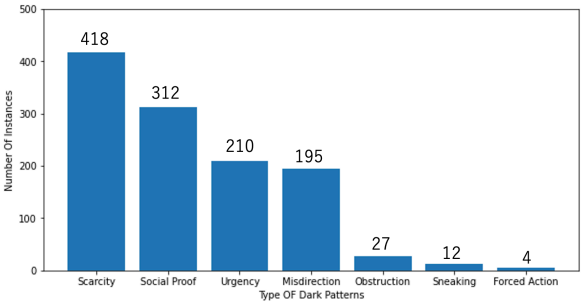

図 2　ダークパターンの種類毎の分布

次に負例，すなわちダークパターンではないテキストを準備した．負例のテキストデータは，Mathur らがダークパターンとして収集したテキストデータを持つサイトから，ダークパターンではないテキストをクローリングにより収集した．表 5 に 10,602 件のテキストデータの単語数に関する統計量を示す．

表 5　ダークパターンに該当するテキストの単語数に関する統計量

平均値	標準偏差	最小値	中央値	最大値
5.84	1.84	4	5	10

収集の手順について述べる．まず，Mathur らがダークパターンを収集したサイトの URL にアクセスし，HTTP のレスポンスが 200 番台であるサイトの HTML をダウンロードした．ダウンロードした HTML から，HTML エレメント単位で，テキストデータのみを抽出する．次に，抽出したテキストデータを'.' で分割することによって，センテンス単位に分割した．次に，単語数が 4 以上 11 未満のテキストのみを抽出した．以上の手順によって，得られたテキストデータの総数は 47,510 件である．

得られた 47,510 件のテキストデータから 10,602 件のテキストデータをランダムに抽出し，これらのテキストデータをショッピングサイトにおけるダークパターンではないテキストデータとした．

表 6　テキストデータ各種類の具体例 (ダークパターンではないテキストを「Not Darkpattern とする)

種類	具体例
Scarcity	Only 2 units left in stock
Social Proof	9 people are viewing this.
Urgency	Your order is reserved for 09:45 minutes!
Misdirection	No, I'll rather pay full price.
Obstruction	To cancel your order before it ships, call us.
Sneaking	Purchase protection added
Forced Action	I agree to receive marketing emails from Natural Life
Not Darkpattern	See our Delivery Policy

4.3 LightGBM，SVM によるダークパターンの自動検出モデル

LightGBM [8] および線形 SVM を用いた機械学習モデルの概要図を図 3 に示す．

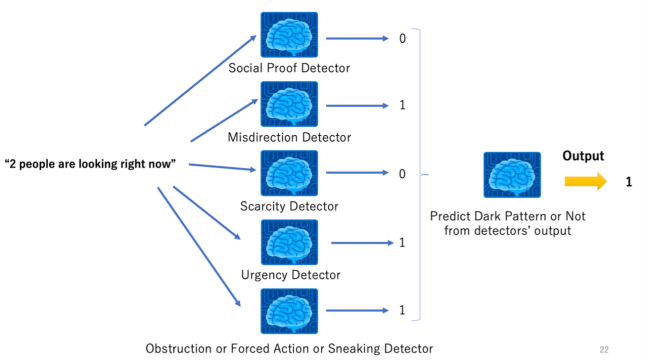

図 3　アンサンブル学習によるダークパターン判定

図中の Detector として，LightGBM あるいは線形 SVM を用いてアンサンブル学習を実現している．それぞれの種類のダークパターンのテキストデータとダークパターンではないテキストデータを用いて，その種類のダークパターンを検出する検出器を各種類に対して実装した．ただし，Obstruction, Forced Action, Sneaking に関しては，図 2 で示した通り，データ数が少ない．そのため，それらは一つの種類としてまとめ，Obstruction・Forced Action・Sneaking のダークパターンに該当するテキストかそうでないかを判定するモデルとしている．

それぞれの種類に対する合計 5 つの検出器から得られた出力を入力とした機械学習モデルから得られる出力を，最終的な出力とすることでアンサンブル学習を実現している．なお，各種類のダークパターンを検出する検出器およびそれらの出力を入力として最終的な出力を行う．機械学習モデルは，ダークパターン毎に用意した学習器と同じモデルを用いている．すなわちダークパターン毎の学習器として LightGBM を用いた場合は，LightGBM を，線形 SVM をダークパターン毎のモデルとして用いた場合は，線形 SVM を用いている．

4.4 BERT によるダークパターンの自動検出モデル

BERT(Bidirectional Encoder Representations from Transformers) [9] は Devlin らによって提案された手法で，テキスト分類，質問応答といった広範囲の自然言語処理タスクで State-of-the-art (SOTA) を達成している言語モデルである．

BERT はその中間層において，12 層の Transformer の Encoder 部分を重ねる構造をしたモデルである．マスク穴埋め問題 (Masked language modeling)，次文予測 (Next sentence prediction) によって事前学習されたモデルを，4.2 節で説明したデータセットによって fine-tuning することで，学習を行なった．

モデルの概要図を図 4 に示す．本提案手法では，12 層の隠れ層 (Transformer) を持ち，次元数が 768 の BERT の基本モデルを利用する．図の NN 部分には，BERT が出力した CLS の

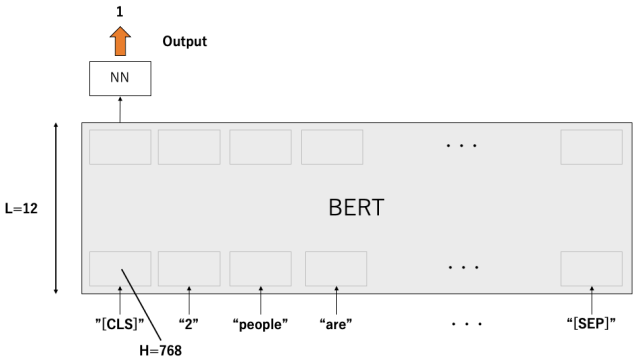

図 4　BERT によるモデルの概要図

埋め込み表現を 2 次元ベクトルに線形変換する全結合層を利用する．

5 評価実験

5.1 LightGBM，SVM による自動検出モデルの評価結果

特徴量の抽出手順について述べる．まず，テキストを 1-gram,2-gram,3-gram のそれぞれを用いて Bag-of-Words で表現する．それにより，テキストに対する 3 種類の分散表現が得られる．それらを結合することによって，得られたベクトルをテキストの特徴量としている．

LightGBM，SVM のそれぞれに対し，5 分割交差検証によって，評価を行った．評価結果を表 7 に示す

表 7　LightGBM，SVM による 5 分割交差検証を用いた自動検出モデルの評価結果

	F 値	適合率	再現率	精度
線形 SVM	0.880	0.820	0.952	0.978
LightGBM	0.866	0.820	0.918	0.975

5.2 BERT による自動検出モデルの評価結果

事前学習済みモデルとして，Hugging Face[2]が公開しているライブラリである Transformers[3]から，BERT-base (bert-base-uncased) を利用した．また，fine-tuning の設定として，最大入力系列長を 24token，バッチサイズは 128，エポック数は 10，学習率 1×10^{-5}，最適化手法には Adam を用いた．評価結果を表 8 に示す

表 8　BERT による自動検出モデルのテストデータに対する評価結果

F 値	適合率	再現率	精度
0.962	0.952	0.972	0.989

2：https://huggingface.co
3：https://github.com/huggingface/transformers

6 おわりに

本稿では，インターネットサービス上のダークパターンからユーザを保護することを目的として，ダークパターンの自動検出に関する実験・評価を行った．ショッピングサイトにおけるダークパターンに該当するテキストとショッピングサイトにおけるダークパターンに該当しないテキストを用いて，SVM，勾配ブースティング，BERT によるショッピングサイトにおけるダークパターンの自動検出モデルを構築・評価した．その結果，BERT を用いることで F 値として 0.962 を得た．

謝辞 本研究は，LINE 株式会社との共同研究によるものである．

参考文献

[1] A.Mathur,G.Acar,M.Friedman,E.Lucherini,J.Mayer,M.Chetty and A.Narayanan,Dark Patterns at Scale: Findings from a Crawl of 11K Shopping Websites, Proc. ACM Hum.-Comput. Interact,Article 81,(2019).

[2] A.Mathur,M.Kshirsagar and J.Mayer,What Makes a Dark Pattern... Dark?: Design Attributes, Normative Considerations,and Measurement Methods, Proceedings of the 2021 CHI Conf. on Human Factors in Computing Systems,Article 360,(2021).

[3] A.Mathur,A.Narayanan and M.Chetty,Endorsements on Social Media: An Empirical Study of Affiliate Marketing Disclosures on YouTube and Pinterest, Proc. ACM Hum.-Comput. Interact.,Article 119,(2018).

[4] B.Harry,Dark Patterns.,https://darkpatterns.org/,(2018), Accessed on 12/26/2021.

[5] California Secretary of State.,Qualified Statewide Ballot Measures.,https://www.oag.ca.gov/system/files/initiatives/pdfs/19-0021A1%20%28Consumer%20Privacy%20-%20Version%203%29_1.pdf,(2020),Accessed on 12/17/2021.

[6] C.Graym,Y.Kou,B.Battles,J.Hoggatt and A.Toombs,The Dark (Patterns) Side of UX Design,Proceedings of the 2018 CHI Conf. on Human Factors in Computing Systems,pp.1-14,(2018).

[7] G.Di,L.Braz,E.Fregnan,F.Palomba and A.Bacchelli,UI Dark Patterns and Where to Find Them: A Study on Mobile Applications and User Perception,Proceedings of the 2020 CHI Conf. on Human Factors in Computing Systems, pp.1-14,(2020).

[8] G.Ke,Q.Meng,T.Finley,T.Wang,W.Chen,W.Ma,Q.Ye and T.Liu ,LightGBM: A Highly Efficient Gradient Boosting Decision Tree, Proceedings of the 31st Int'l Conf. on Neural Information Processing Systems,pp.3149 – 3157,(2017).

[9] J.Devlin,M.Chang,K.Lee and K.Toutanova,BERT: Pre-training of Deep Bidirectional Transformers for Language Understanding.,Proc. of NAACL-HLT 2019,pp.4171-4186,(2019).

[10] K.Bongard-Blanchy,R.Arianna,R.Salvador,D.Sophie,K.Vincent and L.Gabriele,I Am Definitely Manipulated, Even When I Am Aware of It. It's Ridiculous! - Dark Patterns from the End-User Perspective.,Designing Interactive Systems Conf. 2021,pp.763 – 776,(2021).

[11] M.Nouwens,I.Liccardi,M.Veale,D.Karger and L.Kagal,Dark Patterns after the GDPR: Scraping Consent Pop-Ups and Demonstrating Their Influence.,Proceedings of the 2020 CHI Conf. on Human Factors in Computing Systems, pp.1-13,(2020).

[12] National Commission on Informatics and Liberty (CNIL).,Shaping Choices in the Digital World.,https://linc.cnil.fr/sites/default/files/atoms/files/cnil_ip_report_06_shaping_choices_in_the_digital_world.pdf,(2020), Accessed on 12/28/2021

[13] Organisation for Economic Co-operation and Development.,Summary of discussion,Roundtable on Dark Commercial Patterns Online,https://www.oecd.org/officialdocuments/publicdisplaydocumentpdf/?cote=DSTI/CP(2020)23/FINAL&docLanguage=En,(2020),Accessed on 12/28/2021.

[14] T.Soe,O.Nordberg,F.Guribye and M.Slavkovik,Circumvention by Design - Dark Patterns in Cookie Consent for Online News Outlets.,Proceedings of the 11th Nordic Conf. on Human-Computer Interaction: Shaping Experiences,Shaping Society, New York,pp.1-12.(2020).

[15] T.Mildner and S.Gian-Luca.,Ethical User Interfaces: Exploring the Effects of Dark Patterns on Facebook.,Extended Abstracts of the 2021 CHI Conf. on Human Factors in Computing Systems,Article 464,(2021).