Welchen Einfluss haben Dark Patterns auf Nutzer?

Karhan, Marvin
Hochschule Mannheim
Fakultät für Informatik
Paul-Wittsack-Str. 10, 68163 Mannheim

***Zusammenfassung*—Dark Patterns sind Negativbeispiele für Interface-Design. Sie nutzen Tricks, um die Entscheidungen von Nutzern zu manipulieren. Die menschliche Psyche ist anfällig für diese Tricks und obwohl in den letzten Jahren Gesetzgeber immer mehr versuchen, den Einfluss von Dark Patterns zu reduzieren, setzen Unternehmen sie weiter ein, um die Entscheidungen ihrer Nutzer zu manipulieren. Nutzer müssen Dark Patterns erkennen können, um ihren Einfluss zu verstehen und sich vor ihnen zu schützen. Wenn genügend Nutzer Dark Patterns erkennen und Unternehmen, die sie einsetzen meiden, haben diese Unternehmen keinen Anreiz mehr sie einzusetzen.**

Inhaltsverzeichnis

1. Einleitung

Mit der immer stärker zunehmenden Digitalisierung und der steigenden Anzahl an Internetnutzern [1], wird der Einfluss von Applikationen im Internet und ihrem Design immer größer. Für Nutzer ist es nicht immer klar, wenn sie ausgenutzt wurden.

Menschen sind besonders gut in der Erkennung von Mustern. Sie nutzen die Muster verschiedener Laute, um Sprache zu verstehen und sprechen zu können. Es ist wichtig zu verstehen, welche manipulativen Muster im Internet eingesetzt werden, denn Design ist die Sprache des Internets [2].

Viele Gelehrte befassen sich damit, Richtlinien und Vorlagen für gutes Interface-Design zu verfassen. Dieses Paper beleuchtet die dunkle Seite des Interface-Designs im Webumfeld. Von besonderer Bedeutung ist dabei der Einfluss von *Dark Patterns* auf Nutzer. Sie sind Negativbeispiele für Interface-Design und dienen nicht dem Wohle der Nutzer. Harry Brignull [3] gilt als der Begründer des Dark Pattern Begriffs und definiert ihn als Tricks, die Nutzer dazu überzeugen, etwas zu tun, was sie ursprünglich nicht tun wollten. Sie nutzen psychologische Mechanismen, um die Entscheidungsfindung des Nutzers wesentlich zu beeinflussen.

Diese Arbeit bietet einen Einblick in die Konzepte, die das Fundament für Dark Patterns bilden und welche Rolle dabei psychologische Mechanismen spielen. Außerdem werden Beispiele von Dark Patterns in die von Gray, Kou, Battles, Hoggatt und Toombs [4] etablierte Taxonomie eingeordnet und bewertet. Zudem werden legislative Maßnahmen gegen Dark Patterns betrachtet und die Frage, wieso die Aufklärung von Designern und Nutzern nötig ist, beantwortet.

Es wird die von Gray et al. [4] vorgeschlagene Taxonomie verwendet, weil sie aktuell ist, anders als die vergleichbare Taxonomie von Conti und Sobiesk [5] und sich nicht auf eine Domäne konzentriert wie die Taxonomien von Lewis [6] im Bereich mobiler Anwendungen.

Das Ziel dieser Arbeit ist zweiseitig, einerseits soll es Designern leichter fallen, Dark Patterns in ihren Designentscheidungen zu vermeiden und anderseits sollen Nutzer leichter in der Lage sein, Dark Patterns zu erkennen, um so negative Konsequenzen zu vermeiden. Ziel dieses Papers ist nicht, eine eigene Taxonomie zu erstellen oder eine vollständige Auflistung aller existierenden Dark Patterns zu bieten.

2. Dark Patterns Grundlagen

Traditionell nutzen Firmen Plakate und Anzeigen, um Kunden auf sich aufmerksam zu machen. Durch die Entstehung des Internets verbreitete sich das sogenannte *Growth Hacking*. Mit Growth Hacking werden Marketingaktionen bezeichnet, welche Tricks ausnutzen, um Wachstum zu steigern. Growth Hacks bewegen sich häufig an der Grenze zum Illegalem [7]. LinkedIn gab seinen Nutzern die Möglichkeit, automatisiert persönliche Kontakte per E-Mail zu LinkedIn einzuladen. LinkedIn versuchte an acht Stellen diese Einwilligung zu erhalten und nutzte dafür zusätzlich Dark Patterns [8]. Die

erhaltenen Daten wurden verwendet, um wiederholt E-Mails im Namen der Nutzer an deren Kontakte zu senden. Daraus resultierte eine Sammelklage, da es für die Nutzer nicht klar war, dass LinkedIn die Kontakte im Namen des Nutzers mit Werbemails spammen würde [9]. Solche Marketingaktionen sind der Ursprung von Dark Patterns.

Dieses Kapitel ordnet Dark Patterns ein und beschreibt, wie die menschliche Psyche ausgenutzt werden kann, was *Nudging* ist und anhand eines Beispiels wie *Nudges* eingesetzt werden können.

2.1. Anti-Pattern

Pattern sind der Bauplan einer Lösung zu einem wiederkehrenden Problem. Sie existieren in vielen Anwendungsbereichen [10, S. 1].

Anti-Pattern ist ein Sammelbegriff für Pattern, welche wiederkehrende Lösungen liefern und dabei mehr Probleme erzeugen als lösen [10, S. 193-195]. Wie sich aus dem Namen bereits erschließen lässt, sind Dark Patterns eine spezifische Pattern-Art.

Unternehmen setzen Dark Pattern ein, um ihre Reichweite zu erhöhen. Das schafft Probleme aufseiten der Nutzer, da sie ausgenutzt werden und Profit über Nutzerfreundlichkeit gestellt wird [11]. Deshalb zählen Dark Patterns zu der Familie der Anti-Pattern.

2.2. Psychologie

Dark Patterns nutzen psychologische Mechanismen aus, um Nutzer zu bewegen, etwas ungewollt oder unbewusst zu tun [3]. Dafür nutzen sie oft kognitive Verzerrung, nutzen also mit speziellen Techniken die Denkweise unseres Gehirns aus [12].

Eine weitverbreitete Technik im Einzelhandel ist die psychologische Preisgestaltung. Das heißt, der Preis eines Produkts wird knapp unter einer runden Zahl angesetzt. Diese Technik ist schon seit mehreren Jahrzehnten im Einsatz und laut Bizer und Schindler (2005) [13] ein effektives Mittel zur Verkaufssteigerung. Im Gegensatz dazu steht Wieseke, Kolberg und Schons [14] Studie aus dem Jahr 2015, die sagt: Runde Preise sorgen für die höchstmögliche Verkaufswahrscheinlichkeit, da diese bequemer für den Käufer sind. Ein vergleichbarer Effekt kann bei Dark Patterns auftreten. Im ersten Schritt sorgt der Einsatz von Dark Patterns für eine höhere Nutzerbindung, jedoch im zweiten Schritt zu einer gegenläufigen Wirkung [15].

Schon in der Zeit vor der digitalen Revolution wurden die Effekte kognitiver Verzerrung untersucht. Die Ergebnisse dieser Untersuchungen geben Aufschluss über die Manifestierung von Dark Patterns in der menschlichen Psyche.

Tversky und Kahneman [16] zeigen in ihrer Untersuchung des Framing-Effekts, wie die Darstellung eines Problems das Ergebnis beeinflusst: Probanden treffen eine andere Auswahl, obwohl sich nur die Darstellung des Problems geändert hat. Konkret mussten die Probanden im ersten Problem konsekutiv eine aus zwei Möglichkeiten wählen. Dabei handelte es sich um die Chance, Geld zu gewinnen oder zu verlieren. In einem anderen Problem wurden die zwei meistgewählten sowie die zwei übrigen Optionen zusammengefasst. Nach der Kombination der zwei Aussichten entschieden sich 100% auf die vorher kaum gewählten Optionen. Diese psychologische Betrachtung lässt sich leicht auf Dark Patterns ausweiten, da Designer in einem Webumfeld weitreichende Möglichkeiten haben, um Informationen so zu vermitteln, dass der Nutzer durch ihre Darstellung zu einer anderen Entscheidung gedrängt wird.

2.3. Nudging

Richard H. Thaler ist Nobelpreisträger für Wirtschaftswissenschaften. Er ist zusammen mit Cass R. Sunstein der Autor des Buchs *Nudge: Improving Decisions About Health, Wealth, and Happiness* [17], der den Begriff *Nudge* geprägt hat.

Er bezeichnet Personen, die Macht über den Kontext haben, indem Andere Entscheidungen treffen als *choice architects* [17, S. 3]. Im Fall von Dark Patterns sind meistens Designer diejenigen, die Thaler und Sunstein als *choice architects* bezeichnen. Ihre Werkzeuge sind die psychologischen Effekte und Techniken.

To nudge bedeutet im herkömmlichen Sinne, jemanden sachte berühren oder schubsen [18]. Wir werden den Begriff wie Thaler und Sunstein im übertragenen Sinne nutzen, wobei *nudge* meint, jemanden mithilfe kleiner Anreize zu einem wünschenswerten Ziel zu drängen. Denn schon mit nur kleinen Anreizen kann der Nutzer zu einer anderen Entscheidung gedrängt werden [7].

Abbildung 1. Eigene Aufnahme des Tracking-Banners der Hochschule Mannheim [19]

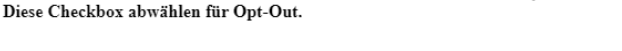

Abbildung 2. Eigene Aufnahme der Tracking-Opt-out-Checkbox der Hochschule Mannheim [19]

Um *Nudging* besser zu verstehen, betrachten wir ein Dark Pattern, welches sich auf der Homepage der Hochschule Mannheim finden lässt. In Abbildung 1 ist ein Ausschnitt des Tracking-Banners der Hochschule Mannheim zu sehen. Die Zustimmung zu nicht essenziellem Tracking wird hinter einem prominent dargestelltem *Weiter* Button verborgen. Um eine konträre Entscheidung zu treffen, muss der Nutzer auf den weit weniger prominenten *hier* Link klicken. Dieser führt zu der Datenschutzerklärung der Hochschule, in der nach der in Abbildung 2 dargestellten Checkbox gesucht werden muss, um das Tracking zu deaktivieren. Auffällig ist, dass in dem Text das Wort *tracking* nicht vorkommt. Hier wurden mehrere *Nudges* genutzt, um den Nutzer dazu zu bewegen, das Tracking zu akzeptieren. Erst wird der Nutzer zum direkten Akzeptieren durch einen auffälligeren Button *genudged*, danach wird der Nutzer durch das erschwerte Abwählen des Trackings in Richtung der Akzeptanz des Trackings *genudged*.

Zusammenfassend lässt sich sagen, dass Dark Patterns als Zusammenschluss verschiedener Nudges verstanden werden kann.

3. Kategorien von Dark Patterns

Der Ansatz von Gray et al. [4] nutzt Brignulls [3] Taxonomie, die primär als Resultat verschiedener Beispiele entstanden ist, und kombiniert sie, zusammen mit eigens definierten Dark Patterns in Kategorien. Die Kategorisierung basiert auf den Beweggründen, welche Designer mit dem Einsatz der Dark Patterns haben.

Der Ansatz von Gray et al. [4] eignet sich gut für das Ziel dieses Papers, da durch ihre Kategorisierung der Bogen von der Intention der Designer zu den Auswirkungen auf den Nutzer geschlagen werden kann, ohne dabei auf jedes einzelne Dark Pattern einzugehen. Es ist nicht wichtig, dass der Leser jedes Dark Pattern auswendig kann. Zudem können Design Elemente oft mehreren Dark Patterns und/oder Kategorien zugeordnet werden.

Jede Kategorie wird kurz erläutert und mithilfe eines repräsentativen Beispiels/Beispielen für ein Dark Pattern genauer betrachtet. Dabei wird herausgestellt, welche Faktoren wichtig für die Erkennung des Dark Patterns sind.

Ziel dieses Abschnittes ist es, dass der Leser potenzielle Dark Patterns leichter erkennt und einordnen kann, um sich dadurch besser vor ihnen schützen zu können.

3.1. Nagging

Nagging Dark Patterns zeichnen sich durch minimale Abweichungen der erwarteten Funktionsweise, über eine oder mehrere Interaktionen, aus [4].

Abbildung 3. Eigene Aufnahme eines Rabatt-Pop-ups von g-star.de [20]

In Abbildung 3 ist ein Rabatt-Pop-up von g-star.de zu sehen. Es erscheint zum ersten Mal direkt nach dem Akzeptieren der Cookies und dann nach unbestimmter Zeit wieder, in leicht abgewandelter Form. Ziel ist es, an die E-Mail-Adresse des Nutzers zu gelangen. Dieses Dark Pattern ist wie alle Nagging Dark Pattern mit dem Zwang verbunden, dass der Nutzer damit interagieren muss [4].

Vor allem bei mobilen Applikationen muss auf Nagging Dark Patterns geachtet werden. Dort sind sie die häufigst vertretene Dark Pattern Kategorie [21].

3.2. Obstruction

Obstruction Dark Patterns sorgen dafür, das Aktionen schwerer sind als sie sein müssten, mit dem Hintergedanken den Nutzer davon abzubringen, die Aktion abzuschließen [4].

Wer einen Amazon-Account besitzt weiß, wie einfach es ist, einen solchen zu erstellen. Es sind nur wenige Klicks nötig und der Ablauf ähnelt stark anderen Shopping-Webseiten. Will der Nutzer seinen Account löschen, ist das weit schwieriger. Die meisten Nutzer werden versuchen, unter *Mein Konto* ihren Account zu löschen, aber keiner der Links dort gibt dem Nutzer diese Möglichkeit. Um einen Amazon-Account zu löschen, ist es erforderlich, die Amazon Kundenservice Webseite aufzurufen, dort unter *Hilfethemen durchsuchen*, *Datenschutz* anklicken und darunter *Kontaktieren Sie uns* auswählen. Danach öffnet sich eine neue Seite, in der *Fragen zum Datenschutz* angeklickt werden muss, wodurch sich eine neue Seite öffnet, auf der in einem ersten Dropdown *Datenschutzauskunft* und in einem zweiten Dropdown *Konto schließen und Daten löschen* selektiert werden muss. Schließlich kann, nachdem Amazon aufzählt, welche Produkte und Services ohne einen Amazon-Account nicht mehr nutzbar sind, der Account geschlossen werden. Alternativ kann im letzten Schritt die Information über die Konsequenzen einer Accountschließung per E-Mail beantragt werden und über eine Antwort per Mail der Account geschlossen werden. Das ist ein Beispiel für Brignulls Dark Pattern *Roach Motel*, eine Situation, die einfach zugänglich ist, aber aus der es schwer ist, wieder herauszukommen [3]. Wie die Untersuchung des Facebook-Account Deaktivierungsprozesses zeigt, benötigen Nutzer mit Nutzung der Googlesuchfunktion vier- bis achtmal so lange, wie es normalerweise dauern sollte, um die durch das Dark Pattern erschwerte Aktion durchzuführen [15].

Der Zweck davon ist, es dem Nutzer möglichst schwer zu gestalten, eine ungewollte Aktion aus Sicht der Webseiten-Betreiber durchzuführen. Dies resultiert in mehr Macht und Profit aufseiten der Unternehmen.

Das Roach Motel Dark Pattern beruht auf keiner kognitiven Verzerrung [12], es hilft nicht, aktiv auf dieses Dark Pattern zu achten, um es vermeiden zu können. Zudem gibt es auch keine anderen Faktoren, die maßgeblich zur Erkennung dieses Patterns führen. Das führt dazu, dass es das von Nutzern am seltensten erkannte Dark Pattern ist [15].

3.3. Sneaking

Sneaking Dark Patterns versuchen Informationen zu verbergen, zu verschleieren oder zu verzögern, die für den Nutzer relevant sind [4].

In Abbildung 4 werden zwei Ausschnitte der amerikanischen airbnb Webseite gezeigt. Links ist die Kartenansicht von airbnb zu sehen. Auf ihr kann der Nutzer alle verfügbaren Objekte, die in der Region buchbar sind mit ihrem Preis pro Nacht sehen. Auf der rechten Seite der Abbildung 4 ist die Preisdetailansicht des in der Karte ausgewählten Zimmers zu sehen. In der Kartenansicht sind Zusätzliche Kosten wie die *Reinigungsgebühr* und die *Service-Gebühr* nicht offengelegt. Das ist ein Fall des *Hidden Costs* Dark Patterns von Brignull [3], da hier wichtige Information für den Nutzer später als nötig preisgegeben wurden.

Die versteckten Zusatzkosten variieren von Objekt zu Objekt, sodass ein Preisvergleich verschiedener Objekte

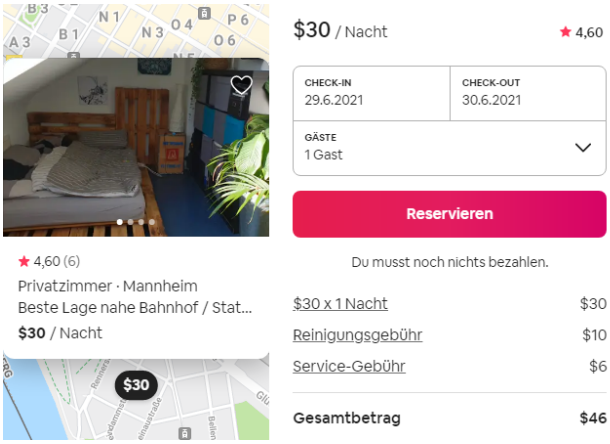

Abbildung 4. Eigene Aufnahme von airbnb.com, links die Kartenansicht und rechts die Detailansicht [22]

über die Kartenansicht für den Nutzer nutzlos ist. Der Nutzer müsste sich jedes Objekt in der Detailansicht anschauen und sich die Preise merken, um sie miteinander zu vergleichen. Zusätzlich werden die versteckten Kosten unter dem Reservierungs-Button angezeigt und fallen dem Nutzer vor der Reservierung nicht auf.

3.4. Interface Interference

Als Interface Interference Dark Pattern zählt jede Manipulation der Benutzeroberfläche, die bestimmte Aktionen gegenüber anderen bevorteilt und dadurch den Nutzer verwirrt oder die Sichtbarkeit wichtiger Handlungsmöglichkeiten einschränkt [4].

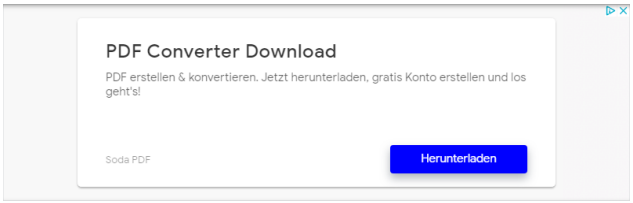

Abbildung 5. Eigene Aufnahme einer Werbeanzeige auf chip.de von Google AdSense [23]

In Abbildung 5 ist eine Werbeanzeige der Webseite chip.de, die über Google AdSense angezeigt wird, abgebildet. Sie wird direkt über dem Download einer PDF-Leseanwendung gezeigt. Das Drücken des *Hernunterladen-Buttons* führt zu der Seite eines Dritten. Hierbei handelt es sich um das von Brignull [3] definierte Dark Pattern *Disguised Ads*, Werbung die sich als Inhalt oder Navigationselement ausgibt, um häufiger angeklickt zu werden.

Die Werbung aus Abbildung 5 wird ganz oben auf der Webseite, vor dem tatsächlich gesuchten Download angezeigt und nutzt den in Unterabschnitt 2.2 beschriebenen Framing-Effekt, um dem Nutzer ein Produkt zu vermitteln, das er nicht sucht. Nutzer, die schon Erfahrung mit Disguised Ads gemacht haben und durch sie Frustration erfahren haben, sind besser darin sie zu erkennen [15].

Bei Interface Interference Dark Patterns wird außerdem oft mit versteckten Informationen und vorausgewählten Standardwerten gearbeitet [4]. Deshalb ist es für diese Kategorie von Dark Patterns wichtig, dass der Nutzer weiß, wo er nach der Information suchen muss und sortieren kann, was für ihn wichtig ist. Je häufiger der Nutzer Interface Interference Dark Patterns begegnet, desto einfacher ist es, sie zu erkennen und zu vermeiden [15].

3.5. Forced action

Forced Action Dark Patterns umfassen jede Situation, in der Benutzer eine bestimmte Aktion ausführen müssen, um auf (oder weiterhin auf) eine bestimmte Funktionalität zugreifen zu können. Diese Aktion kann ein erforderlicher Schritt oder eine Option sein, die als großer Nutzen für den Nutzer getarnt ist [4].

Das in Abschnitt 2 erwähnte LinkedIn Dark Pattern wird von Brignull [3] als *Friend Spam* eingeordnet und von Gray et al. [4] unter dem Begriff *Social Pyramid* subsummiert. Nutzer müssen hier vor allem bei Social-Media-Anbietern aufpassen, ihre Kontakte der Seite zu teilen, da das wie im Fall von LinkedIn im ersten Schritt immer als Vorteil getarnt ist. Die Nutzer wissen nicht und haben keine Kontrolle darüber, was mit diesen Daten passiert.

Abbildung 6. Eigene Aufnahme des spiegel.de Consent-Pop-ups [24]

Facebook hat sich einen besonderen Namen in dieser Dark Pattern Kategorie geschaffen. Durch ihren Gründer und CEO Mark Zuckerberg in Form des Dark Pattern *Privacy Zuckering* von Brignull [3]. Es geht dabei darum, mehr Informationen über sich zu teilen als beabsichtigt. Abbildung 6 ist ein Beispiel für ein Privacy Zuckering Dark Pattern. In dem Consent-Pop-up von spiegel.de hat der Nutzer keine Möglichkeit, die Webseite kostenlos ohne Tracking durch Dritte zu besuchen. Der Nutzer muss also Tracking und Werbung akzeptieren oder ein Abonnement abschließen.

4. Schutz vor Dark Patterns

In der Fußgängerzone stellen Hütchenspieler ihrem Publikum hohe Gewinnchancen in Aussicht. Naive Passanten verstehen es als Geschicklichkeitsspiel dessen Ausgang sie durch ihr Können bestimmen, jedoch ist das ein Irrtum. Der Hütchenspieler nutzt einfache Taschenspielertricks und kontrolliert jederzeit den Ausgang des Spiels. Das Webumfeld bietet deutlich mehr Werkzeuge, um Nutzer in die Irre zu führen, sodass es nahezu unmöglich ist, für einen Nutzer sämtliche Dark Patterns

zu erkennen [15]. Dazu kommt, dass Nutzer nicht jedes Wort auf einer Webseite lesen. Sie überfliegen und machen Annahmen [3]. Firmen können das ausnutzen, indem sie die Seite anders aussehen lassen, als was sie tatsächlich aussagt [3].

Um Nutzer zu schützen, gibt es zwei Möglichkeiten. Entweder wird der Einsatz von Dark Patterns durch den Staat reguliert oder Nutzer erkennen Dark Patterns und vermeiden Unternehmen, die diese einsetzen und regulieren den Einsatz von Dark Patterns auf diese Weise [7].

Das Erkennen von Dark Patterns ist ebenso wichtig für Designer wie für Nutzer. Sie entscheiden, ob Dark Patterns in einer Webseite vorhanden sind. Es kann sein, dass Designer A/B-Testing einsetzen und dadurch ohne es zu wissen, Dark Patterns in ein Design einfügen [7].

4.1. Gesetzliche Einschränkungen

Gesetzliche Einschränkungen sind wichtig. Ohne sie können Unternehmen Dark Patterns uneingeschränkt einsetzen und so Nutzer ausnutzen. Grade Dark Patterns der Kategorien Nagging und Obstruction werden selten von Nutzern erkannt [4, 15], deshalb können sie von Unternehmen eingesetzt werden, ohne ihre Nutzer dabei zu verärgern.

In diesem Paper wurde definiert, was Dark Patterns sind und wie sie zu erkennen sind. Nun stellt sich die Frage, wie Dark Patterns im Gesetz definiert sind. Der amerikanische Bundesstaat Kalifornien hat in seinem im November 2020 verabschiedeten Gesetz unter Cal. Civ. Code § 1798.140(l) (Teil des California Consumer Privacy Act (CCPA)) Dark Patterns als Benutzeroberflächen, die designt oder manipuliert wurden, mit dem Effekt, dass die eigenständige Entscheidungsfindung oder Wahl des Nutzers wesentlich untergraben oder beeinträchtigt wird, definiert.

Das ist eine sehr weit gefasste Definition, die Raum für Interpretation lässt und es den regulierenden Institutionen schwer macht, gegen rechtliche Verstöße durchzugreifen. Diese Annahme hat sich schon in Bezug auf andere Gesetze für wahr erwiesen. Die im Mai 2018 in Kraft getretene europäische Verordnung (EU) 2016/679 (Datenschutz-Grundverordnung (DSGVO)), die unter anderem Webseiten auffordert, Besucher ihrer Seite um Erlaubnis zu fragen, bevor sie personenbezogene Daten als Cookies speichert, sorgt dafür, dass fast jede Webseite den Nutzer nach seiner Erlaubnis fragt, personenbezogene Daten sammeln zu dürfen. Wie eine Studie von Nouwens, Liccardi, Veale, Karger und Kagal [25], die Drittanbieter Software zur Handhabung der DSGVO Regularien mit Consent Management Platforms (CMPs) in 680 Britischen Webseiten untersuchte, zeigt, halten sich nur 11,8% der CMPs an die minimalen Standards der DSGVO. Zudem ergab die Studie, dass Webseiten Dark Patterns einsetzen, um öfter die Einwilligung ihrer Nutzer zu bekommen. Bei Seiten, die den Opt-out-Button von der ersten Seite des Einwilligungsprozesses entfernen, steigt die Anzahl der Nutzer, die einwilligen um 22–23 Prozentpunkte. Das ist ein Obstruction (Unterabschnitt 3.2) Dark Pattern, das zeigt, wie geltende Gesetze Dark Pattern Bildung unterstützt. Eine Studie von Soe, Nordberg, Guribye und Slavkovik [26] untersuchte ebenfalls die Auswirkung der DSGVO in 300 manuell ausgewählten Cookie-Pop-ups in Nachrichtenagenturen und fand dabei in 296 von ihnen Dark Patterns.

Ein weiteres Beispiel der Regulierung zur Verbreitung von Dark Patterns ist das deutsche Gesetz BGBl. I S. 3352 (Netzwerkdurchsetzungsgesetz (NetzDG)), auch Facebook-Gesetz genannt, welches im Oktober 2017 in Kraft getreten ist. Es schreibt unter anderem vor, dass große Soziale Netzwerke eine Möglichkeit bieten müssen, um gesetzwidrige Inhalte melden zu können. Das Bearbeiten von solchen Meldungen kostet Geld. Deswegen nutzen Soziale Netzwerke Dark Patterns, um es Nutzern möglichst schwer zu gestalten, gesetzwidrige Inhalte zu melden [27].

Bei der Beschließung von Gesetzen müssen in Zukunft Interface-Design-Entscheidungen, welche das Gesetz umgehen können oder seine Auswirkungen auf die betroffenen Unternehmen mindert, genauer in Betrachtung gezogen werden. Zudem sollte bei aktuell geltendem Recht wie der DSGVO, die bisher kaum Konsequenzen nach sich zog [25], härter durchgegriffen werden, um so Präzedenzfälle für bösartiges Interface-Design wie Dark Patterns zu schaffen [27].

4.2. Designer-Aufklärung

Der Zweck von Design ist es, Nutzer zu überzeugen, etwas zu tun. Das birgt Potenzial, den Nutzer auszunutzen [28, 29]. Designer sollten besorgt über die Verbreitung von Dark Patterns sein. Sie gelten als unethisch und wirken sich schlecht auf ihre Reputation aus [7].

Designer können für ein bestimmtes Publikum gutartige Entscheidungen treffen, welche aber für ein breiteres Publikum in manipulatives Design münden kann [4]. Entscheidungen, die für ein breites Publikum geschaffen werden, können ebenfalls Dark Patterns produzieren, wie es bei A/B-Tesing der Fall ist. A/B-Testing wird häufig in der Webentwicklung eingesetzt, da so Annahmen mit Daten untermauert werden können [30]. Für A/B-Testing werden häufig Daten verwendet, die wichtig für die Bilanz des Unternehmens sind [30, 7]. Das führt dazu, dass Designer unbewusst und ohne eine böse Absicht Dark Patterns in die Webseite einbinden [7].

Moralisch deutlich bedenklicher sind die Fälle, in denen Designer Dark Patterns bewusst einsetzen, aus eigenem Willen oder durch Druck von Vorgesetzen. Dabei müssen Designer nicht über Dark Patterns, sondern über ihre Folgen bei Nutzern aufgeklärt werden, um entweder an ihre Moral zu appellieren oder darauf, dass sie einen negativen Effekt auf Nutzerbindung und somit auf Profit haben können. Ein weiterer Vorschlag von Gray et al. [4] ist, dass sich Designer ethischen Verordnungen verpflichten, wie es beispielsweise bei Ärtzen der Fall ist.

4.3. Nutzer-Aufklärung

Laut Brignull [3] ist der beste Schutz vor Dark Patterns sie sich bewusst zu machen und die Firmen, die sie benutzen, zu boykottieren. Unterabschnitt 2.2 zeigt, dass der Mensch anfällig für Dark Patterns sein kann. 41.4% der Befragten einer Studie von M. Bhoot, A. Shinde und P. Mishra [15] gaben an, noch nie von einer Webseite ausgetrickst worden zu sein. Keiner der Befragten hatte alle zwölf Dark Pattern, die Gegenstand der Studie waren,

identifizieren können. Dabei wurde Auftrittshäufigkeit als wichtigster Gesichtspunkt zur Identifikation von Dark Pattern erkannt. Deshalb ist es wichtig, Nutzer über Dark Patterns aufzuklären, sodass sie diese leichter erkennen, um sich selbst vor ungewollten Konsequenzen zu schützen.

In den letzen Jahren gewann der Dark Pattern Begriff immer mehr an Bedeutung [11]. Er wurde zum Schlagwort in Massenmedien und der Politik, repräsentativ für manipulatives Interface-Design. Je mehr über Dark Patterns gesprochen wird, desto bewusster werden sie den Nutzern und je mehr Nutzer Dark Patterns erkennen und aus dem Weg gehen, desto weniger effektiv sind sie für Unternehmen. Sobald Dark Patterns sich nicht für Unternehmen rentieren, gibt es keinen Anreiz sie einzusetzen.

5. Fazit und Ausblick

Dark Patterns nutzen psychologische Mechanismen und nudgen den Nutzer hin zu einer Entscheidung, auf die er ursprünglich nicht abzielte. Für Nutzer ist es wichtig, Dark Patterns zu erkennen, um sich vor ihnen zu schützen. Die zwei wichtigsten Faktoren zu ihrer Erkennung sind Auftrittshäufigkeit und Frustration, die im vorherigen Zusammentreffen mit Dark Pattern aufgebaut wurden [15]. Nutzer sollten Unternehmen meiden, die Dark Pattern einsetzen, um ihnen den Anreiz dafür zu nehmen. In Fällen, in denen Nutzer es schwierig haben, Dark Patterns zu erkennen, wie bei den Kategorien Nagging und Obstruction [4, 15], ist es wichtig, dass es Gesetze gibt, die Nutzer vor Manipulation schützen. Leider zeigen aktuelle Gesetze, wie das NetzDG und Richtlinien wie die DSGVO nur für mäßigen Erfolg [25, 26]. Unklar ist, ob es genügt, bei aktuellen Gesetzen stärker durchzugreifen, um Präzedenzfälle für die Zukunft zu schaffen [27] oder ob die aktuelle Auslegung überhaupt genug der Tricks, die Dark Patterns nutzen, abdeckt. In jedem Fall müssen bei der Beschließung zukünftiger Gesetze Dark Patterns mit berücksichtigt werden.

Für Designer ist es ebenfalls wichtig, Dark Patterns zu erkennen, um sie nicht ungewollt, beispielsweise durch den Einsatz von A/B-Tesing, in eine Webseite einzubauen. Der bewusste Einsatz von Dark Patterns durch Designer könnte verhindert werden, indem eine ethische Verordnung eingeführt wird, der sich Designer verpflichten müssen, wie das bei Ärtzen der Fall ist [4].

Diese Arbeit hat nur einen kleinen Teil der existierenden gesetzlichen Regelungen betrachtet. Nachfolgende Arbeiten können sich als Ziel setzen, alle wichtigen Gesetze mit Einfluss auf Dark Patterns zu sammeln und zu untersuchen, wie sich diese auf die Ausbreitung von Dark Pattern auswirken oder welche Gesetze am besten vor Dark Patterns schützen.

Abkürzungen

CCPA California Consumer Privacy Act
CMP Consent Management Platform
DSGVO Datenschutz-Grundverordnung
NetzDG Netzwerkdurchsetzungsgesetz

Literatur

[1] ITU. „Anzahl der Internetnutzer weltweit in den Jahren 2005 bis 2019 (in Millionen)“. (30. Nov. 2020), Adresse: https://de.statista.com/statistik/daten/studie/805920/umfrage/anzahl-der-internetnutzer-weltweit/.

[2] Nerdwriter1. „How Dark Patterns Trick You Online“, YouTube. (29. März 2018), Adresse: https://www.youtube.com/watch?v=kxkrdLI6e6M (besucht am 11. 05. 2021).

[3] H. Brignull. „Dark Patterns“. (2021), Adresse: https://www.darkpatterns.org/ (besucht am 16. 04. 2021).

[4] C. M. Gray, Y. Kou, B. Battles, J. Hoggatt und A. L. Toombs, „The Dark (Patterns) Side of UX Design“, in *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*, ACM, Apr. 2018. DOI: 10.1145/3173574.3174108.

[5] G. Conti und E. Sobiesk, „Malicious interface design“, in *Proceedings of the 19th international conference on World wide web - WWW '10*, ACM Press, 2010. DOI: 10.1145/1772690.1772719.

[6] C. Lewis, *Irresistible Apps*. Apress, 2014. DOI: 10.1007/978-1-4302-6422-4.

[7] A. Narayanan, A. Mathur, M. Chetty und M. Kshirsagar, „Dark Patterns: Past, Present, and Future“, *Commun. ACM*, Jg. 63, Nr. 9, S. 42–47, Aug. 2020. DOI: 10.1145/3397884.

[8] D. Schlosser. „LinkedIn Dark Patterns, or: Why Your Friends KeepSpamming You to Sign Up for LinkedIn“. (5. Juni 2015), Adresse: https://medium.com/@danrschlosser/linkedin-dark-patterns-3ae726fe1462 (besucht am 24. 06. 2021).

[9] A. Strange. „LinkedIn pays big after class action lawsuit over user emails“. (2015), Adresse: https://mashable.com/2015/10/03/linkedin-class-action (besucht am 05. 06. 2021).

[10] D. MacDonald, *Practical UI Patterns for Design Systems*. Apress, 2019. DOI: 10.1007/978-1-4842-4938-3.

[11] S. S. Chivukula, C. Watkins, L. McKay und C. M. Gray, „”Nothing Comes Before Profit”: Asshole Design In the Wild“, in *Extended Abstracts of the 2019 CHI Conference on Human Factors in Computing Systems*, Ser. CHI EA '19, Glasgow, Scotland Uk: Association for Computing Machinery, 2019, S. 1–6. DOI: 10.1145/3290607.3312863.

[12] A. Mathur et al., „Dark Patterns at Scale: Findings from a Crawl of 11K Shopping Websites“, *Proc. ACM Hum.-Comput. Interact.*, Jg. 3, Nr. CSCW, Nov. 2019. DOI: 10.1145/3359183.

[13] G. Y. Bizer und R. M. Schindler, „Direct evidence of ending-digit drop-off in price information processing“, *Psychology and Marketing*, Jg. 22, Nr. 10, S. 771–783, 2005. DOI: 10.1002/mar.20084.

[14] J. Wieseke, A. Kolberg und L. M. Schons, „Life could be so easy: the convenience effect of round price endings“, *Journal of the Academy of Marketing Science*, Jg. 44, Nr. 4, S. 474–494, 2015. DOI: 10.1007/s11747-015-0428-7.

[15] A. M. Bhoot, M. A. Shinde und W. P. Mishra, „Towards the Identification of Dark Patterns: An Ana-

lysis Based on End-User Reactions“, in *IndiaHCI '20: Proceedings of the 11th Indian Conference on Human-Computer Interaction*, Ser. IndiaHCI 2020, Online, India: Association for Computing Machinery, 2020, S. 24–33. DOI: 10.1145/3429290.3429293.

[16] A. Tversky und D. Kahneman, „The framing of decisions and the psychology of choice“, *Science*, Jg. 211, Nr. 4481, S. 453–458, 1981. DOI: 10.1126/science.7455683.

[17] R. H. Thaler und C. R. Sunstein, *Nudge: Improving Decisions About Health, Wealth, and Happiness*. Yale University Press New Haven und London, 2008.

[18] Merriam-Webster, *Nudge*, in *Merriam-Webster.com dictionary*. Adresse: https://www.merriam-webster.com/dictionary/nudge (besucht am 14. 05. 2021).

[19] H. Mannheim, Hochschule Mannheim. (2021), Adresse: https://www.hs-mannheim.de/ (besucht am 14. 05. 2021).

[20] G-Star. (24. Juni 2021), Adresse: https://www.g-star.com/ (besucht am 24. 06. 2021).

[21] L. Di Geronimo, L. Braz, E. Fregnan, F. Palomba und A. Bacchelli, „UI Dark Patterns and Where to Find Them: A Study on Mobile Applications and User Perception“, in *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*, Ser. CHI '20, Honolulu, HI, USA: Association for Computing Machinery, 2020, S. 1–14. DOI: 10.1145/3313831.3376600.

[22] „airbnb“. (2021), Adresse: de.airbnb.com (besucht am 20. 06. 2021).

[23] chip. „Adobe Acrobat Reader DC - Download - CHIP“. (2021), Adresse: https://www.chip.de/downloads/Adobe-Acrobat-Reader-DC_12998358.html (besucht am 20. 06. 2021).

[24] D. Spiegel. (2021), Adresse: https://www.spiegel.de/consent-a- (besucht am 24. 06. 2021).

[25] M. Nouwens, I. Liccardi, M. Veale, D. Karger und L. Kagal, „Dark Patterns after the GDPR: Scraping Consent Pop-Ups and Demonstrating Their Influence“, in *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*, Ser. CHI '20, Honolulu, HI, USA: Association for Computing Machinery, 2020, S. 1–13. DOI: 10.1145/3313831.3376321.

[26] T. H. Soe, O. E. Nordberg, F. Guribye und M. Slavkovik, „Circumvention by Design - Dark Patterns in Cookie Consent for Online News Outlets“, in *Proceedings of the 11th Nordic Conference on Human-Computer Interaction: Shaping Experiences, Shaping Society*, Ser. NordiCHI '20, Tallinn, Estonia: Association for Computing Machinery, 2020. DOI: 10.1145/3419249.3420132.

[27] C. S. Sebastian Rieger. „Dark Patterns: Regulating Digital Design, Wie Regierungen und Regulierungsbehörden auf dieVerbreitung problematischer Benutzerober!ächenreagieren können“. (13. Mai 2020), Adresse: https://www.stiftung-nv.de/en/publication/dark-patterns-regulating-digital-design (besucht am 17. 06. 2021).

[28] H. Oinas-Kukkonen und M. Harjumaa, „Persuasive Systems Design: Key Issues, Process Model, and System Features“, *Communications of the Association for Information Systems*, Jg. 24, 2009. DOI: 10.17705/1cais.02428.

[29] P. Sengers, K. Boehner, S. David und J. '. Kaye, „Reflective design“, in *Proceedings of the 4th decennial conference on Critical computing between sense and sensibility - CC '05*, ACM Press, 2005. DOI: 10.1145/1094562.1094569.

[30] R. Kohavi und R. Longbotham, „Online Controlled Experiments and A/B Testing“, in Jan. 2017, S. 922–929. DOI: 10.1007/978-1-4899-7687-1_891.