Bachelorarbeit

Dark Patterns

Manipulative Benutzererfahrungen im digitalen Raum und deren rechtliche Rahmenbedingungen

Ausgeführt zum Zwecke der Erlangung des akademischen Grades eines

Bachelor of Science

Im Rahmen des Studiums

Software & Information Engineering

unter der Leitung von

Ao. Univ. Prof. Mag. Dr. iur. Univ.

Markus Haslinger

E280 Institut für Raumplanung

Forschungsbereich Rechtswissenschaften

eingereicht an der Technischen Universität Wien

Fakultät für Informatik

von

Anni Chen

Matr.Nr. 11902050

Wien, 13. Juni 2023

_____

Anni Chen

Erklärung zur Verfassung der Arbeit

Hiermit erkläre ich, dass ich diese Arbeit selbständig verfasst habe, dass ich die verwendeten Quellen und Hilfsmittel vollständig angegeben habe und dass ich die Stellen der Arbeit – einschließlich Tabellen, Karten und Abbildungen –, die anderen Werken oder dem Internet im Wortlaut oder dem Sinn nach entnommen sind, auf jeden Fall unter Angabe der Quelle als Entlehnung kenntlich gemacht habe.

Wien, 9. Oktober 2023

_____

Anni Chen

Abstract

Dark Patterns sind ein weit verbreitetes Phänomen, dem Nutzer:innen bei der Internetnutzung immer wieder begegnen. Sie bezeichnen Benutzeroberflächen, die darauf ausgelegt sind, Nutzer:innen zu manipulieren, zu täuschen oder zu bestimmten Handlungen zu zwingen. In der Regel zielen sie darauf ab, mehr Geld, Daten und Aufmerksamkeit von Nutzer:innen zu erlangen, als diese es beabsichtigen oder wünschen. Damit können sich diese manipulativen und irreführenden Benutzeroberflächen negativ auf Nutzer:innen auswirken und ihnen finanzielle Schäden zufügen, ihre Privatsphäre gefährden sowie ein Suchtverhalten bei ihnen auslösen. Insgesamt stellen sie eine Gefahr für die Grundrechte der Nutzer:innen dar.

Das Hauptziel dieser Arbeit ist es, eine umfassende Erläuterung von Dark Patterns zu liefern, um Klarheit in diese Thematik zu bringen. Basierend auf einer Literaturrecherche widmet sich die Arbeit der Untersuchung der Funktionsweise von Dark Patterns, den damit verbundenen Auswirkungen, der Identifizierung von Bereichen, in denen sie auftreten, sowie der Erforschung geeigneter Maßnahmen zur Bekämpfung von Dark Patterns, wobei sowohl rechtliche Aspekte als auch alternative Ansätze betrachtet werden.

Die vorliegende Arbeit zeigt wie komplex Dark Patterns sind. Sie beruhen auf psychologischen Techniken und nutzen menschliche Verhaltensmuster aus, um Nutzer:innen zu unerwünschten Handlungen zu verleiten. Dark Patterns können in verschiedenen Formen auftreten und ihre subtile Natur stellt eine erhebliche Gefahr für die Rechte der Nutzer:innen dar. Um die negativen Auswirkungen von Dark Patterns einzudämmen, ist es wichtig, neben rechtlichen Vorschriften auch Nutzer:innen die nötigen Werkzeuge und Informationen bereitzustellen und Benutzeroberflächen verantwortungsvoll zu gestalten.

Inhaltsverzeichnis

Abkürzungsverzeichnis

ACM	Netherlands Authority for Consumers and Markets
AK	Arbeiterkammer
BMUV	Bundesministerium für Umwelt, Naturschutz, nukleare Sicherheit und Verbraucherschutz
CDR	Corporate Digital Responsibility
CTR	Click-through-rate
DAPDE	Dark Pattern Detection Project
DMA	Digital Markets Act
DSA	Digital Services Act
DSGVO	Datenschutz-Grundverordnung
EDSA	Europäischer Datenschutzausschuss
EG	Europäische Gemeinschaft
EK	Europäische Kommission
EU	Europäische Union
GRC	Charta der Grundrechte der Europäischen Union
ICC	International Chamber of Commerce
KI	Künstliche Intelligenz
OECD	Organisation für wirtschaftliche Zusammenarbeit und Entwicklung
RL	Richtlinie
UGP-RL	Richtlinie über unlautere Geschäftspraktiken
UI	User Interface
UVP	Unverbindlicher Verkaufspreis
UX	User Experience
UXPA	User Experience Professionals Association
VO	Verordnung
VR-RL	Verbraucherrechte-Richtlinie

1 Einleitung

In der heutigen Zeit interagieren wir mehr denn je mit Technologien in nahezu allen Bereichen unseres Lebens. Im Zuge der Digitalisierung wurden zahlreiche traditionelle Dienstleistungen erfolgreich in digitale Formate übergeführt. Dadurch finden viele unserer Aktivitäten zunehmend in der digitalen Umgebung statt: Wir greifen unter anderem auf Online-Plattformen und -Dienste zu, um mit unseren Mitmenschen zu kommunizieren, Informationen zu suchen, Einkäufe zu tätigen, Buchungen durchzuführen und Unterhaltung zu finden. Der Trend zum Online-Einkauf innerhalb der Europäischen Union (EU) wird beispielsweise durch eine Erhebung der EU untermauert. Dabei gaben von den befragten Internetnutzer:innen 74% an, eine Ware oder eine Dienstleistung online gekauft zu haben (Eurostat, 2022).

Mit der fortschreitenden Digitalisierung alltäglicher Aktivitäten wächst für Nutzer:innen auch das Risiko, in der digitalen Umgebung manipuliert und getäuscht zu werden. Eine Beobachtung ist der großflächige Einsatz von sogenannten *Dark Patterns*. Dieser Begriff bezeichnet Benutzeroberflächen, die Nutzer:innen mit Absicht manipulieren, täuschen oder zu Fehlentscheidungen zwingen und hat in den letzten Jahren zunehmend Aufmerksamkeit erlangt. Sie werden überwiegend von Unternehmen zum eigenen Vorteil eingesetzt und können den Konsument:innen finanzielle Schäden zufügen, ihre Privatsphäre gefährden und sogar ein Suchtverhalten hervorrufen.

Einige Dark Patterns weisen Ähnlichkeiten zu traditionellen Geschäftspraktiken auf, die außerhalb der digitalen Umgebung Anwendung finden (Narayanan et al., 2020, S. 69). Allerdings ist die Besorgnis in Bezug auf Dark Patterns größer als bei irreführenden Praktiken in der analogen Welt, da die digitale Umgebung subtilere Möglichkeiten bietet, Menschen zu täuschen und zu manipulieren. Durch die ständige Verfügbarkeit digitaler Medien und die einfache Erreichbarkeit von Online-Plattformen und Diensten, steigt zudem die Wahrscheinlichkeit, Opfer von solchen irreführenden Praktiken zu werden.

Aufgrund der weiten Verbreitung von Dark Patterns und die daraus resultierenden Schäden für Konsument:innen ist es von großer Bedeutung ein umfassendes Verständnis für diese Praktiken und ihre Rechtslage zu erarbeiten. Demnach besteht das Ziel dieser Arbeit darin, eine breite Einführung in die Thematik zu geben und

insbesondere die rechtlichen Aspekte zu beleuchten. Die Arbeit stützt sich dabei auf eine umfangreiche Literaturrecherche, bei der wissenschaftliche Artikel, Fachzeitschriften, Internetdokumente, Berichte und relevante rechtliche Dokumente analysiert wurden.

Zunächst erfolgt eine Erläuterung des Begriffs „Dark Patterns“, begleitet von einer Beschreibung der Beeinflussungsformen Manipulation, Zwang und Irreführung, welche Dark Patterns bewirken (Kapitel 2). Im Anschluss werden die Ursprünge von Dark Patterns untersucht (Kapitel 3). Dieses Kapitel hat ebenfalls zum Ziel, die grundlegenden Konzepte von Dark Patterns zu erläutern, um somit ein besseres Verständnis für ihre genaue Funktionsweise zu schaffen. Weiters wird eine Einführung in die verschiedenen Erscheinungsformen von Dark Patterns gegeben (Kapitel 4). Dabei werden eingangs unterschiedliche Typologien angeführt, gefolgt von einer detaillierten Beschreibung einer spezifischen Typologie. Im Zuge dessen werden konkrete Beispiele genannt, um die verschiedenen Aspekte von Dark Patterns zu veranschaulichen. Darauf aufbauend, werden die Auswirkungen von Dark Patterns behandelt und es wird analysiert, welche Dark Patterns welche Auswirkungen haben (Kapitel 5). Im darauffolgenden Kapitel wird untersucht, wie und in welchem Ausmaß Dark Patterns speziell in den Bereichen des E-Commerce bzw. der Online-Marktplätze, des Online-Tourismus und der sozialen Medien vorkommen (Kapitel 6). Im weiteren Verlauf der Arbeit wird auf die rechtliche Situation von Dark Patterns eingegangen, wobei der Schwerpunkt auf dem europäischen Recht liegt (Kapitel 7). In diesem Zusammenhang werden relevante Gesetzgebungen, wie der Digital Services Act (DSA), der Digital Markets Act (DMA) und die Datenschutz-Grundverordnung (DSGVO) analysiert, um aufzuzeigen inwieweit diese Gesetzgebungen Dark Patterns regulieren. Abschließend werden Abwehrstrategien behandelt, die über die Einhaltung gesetzlicher Vorschriften hinausgehen (Kapitel 8).

2 Definitionen

2.1 Dark Patterns

Der User Experience (UX) Experte Harry Brignull führte im Jahre 2010 erstmals den Begriff *Dark Patterns* ein und bezeichnet diese als „*[…] Tricks angewendet auf Webseiten und Apps, die einen dazu bringen unbeabsichtigte Dinge zu tun, wie etwas zu kaufen oder sich für etwas zu registrieren*“ (Brignull, 2010). Gray et al. (2018, S. 3) sehen Dark Patterns als Benutzeroberflächen, welche mit Hilfe von Erkenntnissen aus der Psychologie entwickelt worden sind, um Benutzer:innen zu bestimmten Handlungen zu verleiten. Dabei haben Designer:innen, die solche Benutzerschnittstellen entwerfen, nicht das Interesse der Benutzer:innen im Auge. Mathur et al. (2019, S. 2) deuten hin, dass solche Design Entscheidungen vermehrt für Online-Plattformen, wie die der sozialen Medien, des Online-Handels, auf mobile Apps und Videospiele, getroffen werden. Sie verstehen unter Dark Patterns „*[…] User Interface Design Entscheidungen, die einen Online-Service begünstigen, indem diese Nutzer:innen zu Entscheidungen zwingen, lenken oder täuschen, welche sie möglicherweise nicht getroffen hätten, wenn sie über alles informiert wären, und die Möglichkeit hätten Alternativen auszuwählen*“ (Mathur et al., 2019, S. 2).

Die bewusste Gestaltung von Benutzeroberflächen, um bestimmte Verhaltensmuster hervorzurufen ist nicht unmoralisch per se. Es wird darauf im UX-Design zurückgegriffen, um unter anderem die erfolgreiche Erledigung der Aufgaben zu fördern, Fehler zu minimieren, die aufgewendete Zeit für eine Aufgabe zu senken und generell ein angenehmes Erlebnis Nutzer:innen bei der Interaktion zu bieten (Conti & Sobiesk, 2010, S. 271). Conti und Sobiesk (2010, S. 271) erklären, dass der Hauptunterschied zwischen gutartigem und bösartigem Design darin liege, dass bei letzterem Designer:innen mit Absicht Interaktionsabläufe so gestalten, sodass die Bedürfnisse der Designer:innen über die der Nutzer:innen gestellt werden.

2.2 Manipulation, Zwang, Irreführung

Dark Patterns beeinflussen Nutzer:innen auf unterschiedliche Weise. Sie können Betroffene manipulieren, irreführen oder zu ungewollten Aktionen zwingen (Narayanan et al., 2020, S. 67). Das Ziel dieses Unterkapitels ist es, die drei verschiedenen Formen der Beeinflussung - Manipulation, Zwang und Irreführung - zu differenzieren.

2.2.1 Manipulation

Der Begriff *Manipulation* hat verschiedene Bedeutungen. Im Allgemeinen bezieht sich Manipulation auf eine gezielte Lenkung oder Kontrolle (Susser et al., 2019, S. 12). In der Medizin bezeichnet Manipulation beispielsweise bestimmte Hangriff-Techniken, die in der manuellen Therapie angewendet werden (Maitland, 1996, S. 19). Im Zuge dieser Arbeit wird nicht die Manipulation von Gegenständen oder Objekten in Betracht gezogen, sondern die Manipulation vom menschlichen Verstand. Konkret geht es um die subtile Einflussnahme auf Entscheidungsprozesse, die durch die Ausnutzung kognitiver Verzerrungen erreicht wird (Susser et al., 2019, 21 f.). Manipulation zeichnet sich dadurch aus, dass sich Betroffene nicht im Klaren darüber sind, wie ihre Handlungen zustande gekommen sind. Zudem sind sie sich nicht dessen bewusst, dass der Manipulator sie für die eigenen Interessen ausnutzt (Susser et al., 2019, S. 17).

2.2.2 Zwang

Bei Zwang wird von Betroffenen ein bestimmtes Verhalten gefordert. Dies wird üblicherweise dadurch erreicht, dass den Betroffenen keine andere Wahl gelassen wird, als den Anweisungen des Gegenübers zu folgen (Susser et al., 2019, S. 15). Dennoch herrscht Transparenz, da den Betroffenen klar ist, welche Konsequenzen ihre Handlungen haben. Sie reagieren auf den Zwang und erfüllen die Forderungen der anderen Person, selbst wenn sie nicht in ihrem eigenen Interesse liegen. Die Betroffenen sind sich bewusst, dass sie gezwungen werden. Im Gegensatz dazu erfolgt Manipulation subtil und unterschwellig (Susser et al., 2019, S. 16).

2.2.3 Irreführung

Eine Person in die Irre zu führen oder anders ausgedrückt, zu täuschen, bedeutet, absichtlich falsche Überzeugungen bei ihr hervorzurufen. Dabei ist sich die Person, die täuscht, bewusst über die Falschheit der dargestellten Information (Cohen, 2018, S. 484). Daher können die Betroffenen nicht damit rechnen, dass ihre Entscheidung die erwartete Konsequenz auslöst. Wenn Personen sich der Falschinformation bewusst wären, würden sie höchstwahrscheinlich ihre Wahl zurückziehen (Susser et al., 2019, S. 21). In dieser Hinsicht ist Täuschung intransparent und wird von Susser et al. (2019, S. 22) als eines der Werkzeuge eines Manipulators betrachtet.

3 Herkunft von Dark Patterns

In diesem Kapitel werden die Ursprünge von Dark Patterns untersucht. Narayanan et al. (2020, S. 69) identifizierten drei Hauptbereiche, die für die Entstehung von Dark Patterns verantwortlich sind: Verhaltensökonomie, traditionelle irreführende Praktiken im Handel und das Konzept des Growth Hackings. Im weiteren Verlauf werden diese drei Bereiche einzeln erläutert.

3.1 Forschung in der Verhaltensökonomie

Die Verhaltensökonomie ist eine Disziplin der Wirtschaftswissenschaften und kombiniert Methoden aus der Psychologie und der Ökonomie. Im Konkreten erforscht sie das menschliche Verhalten in Bezug auf die Entscheidungsfindung in wirtschaftlichen Situationen und berücksichtigt emotionale sowie kognitive Faktoren. Sie steht im Kontrast zu der klassischen Ökonomie, welche die Ansicht vertritt, dass Individuen stets rational, im Eigeninteresse, frei von Emotionen und fehlerfrei handeln (Beck, 2014, S. 9). Angesichts der Kritik an die klassische Ökonomie (Weber & Schäfer, 2017, 568 f.), entstanden in den 1970ern Werke von Kahnemann und Tversky (Tversky & Kahneman, 1974). In ihrer Arbeit gehen sie unter anderem der Frage nach, wie Abweichungen von rationalen Entscheidungen zustande kommen. Sie folgern, dass Heuristiken und Urteilsverzerrungen, welche komplexe Entscheidungen entlasten, unpräzise sein können und damit der Grund für irrationale Entscheidungen sind (Tversky & Kahneman, 1974, S. 1124).

3.1.1 Nudging

Innerhalb der Verhaltensökonomie etablierte sich das Konzept des *Nudging*. Geprägt von Thaler und Sunstein (2020) im Jahre 2008, definieren die beiden Autoren *Nudge* als:

> *[...] Maßnahmen, mit denen Entscheidungsarchitekten das Verhalten von Menschen in vorhersagbarer Weise verändern können, ohne irgendwelche Optionen auszuschließen oder wirtschaftliche Anreize stark zu verändern. Ein Nudge muss zugleich leicht und ohne großen Aufwand zu umgehen sein. Er ist nur ein Anstoß, keine Anordnung*. (Thaler & Sunstein, 2020, S. 15)

Nudging beruht auf der Erkenntnis, dass Menschen zu verzerrten Wahrnehmungen und falschen Annahmen tendieren (Thaler & Sunstein, 2020, S. 34). Für das Zustandekommen dieser Phänomene ist es erstmals wichtig, die Funktionsweise des menschlichen Gehirns zu verstehen. Dafür konzipierte Kahneman (2012, 32 f.) ein Zwei-Systeme Modell. Auf der einen Seite spricht er von System 1, welches für das automatische, schnelle, mühelose Denken, steht. Demgegenüber steht System 2, bei welchem es sich um das langsame und durchdachte Denken handelt (Kahneman, 2012, S. 33). Selbst wenn System 1 oft richtig liegt, unterliegt es dennoch vielen Fehlern. Daraus folgt, dass viele Urteilsfehler auf jener Ebene entstehen. Um also das Verhalten zu beeinflussen, zielt Nudging darauf ab, das System 1 Denken zu aktivieren und das System 2 Denken zu umgehen, da auf der Ebene des automatischen Denkens die Urteilsbildung leichter geformt werden kann (Thaler & Sunstein, 2020, S. 36).

Den Autor:innen nach soll Nudging eine Technik für die von ihnen vorgestellte neue Bewegung, den sogenannten *libertären Paternalismus*, sein (Thaler & Sunstein, 2020, S. 14). Das Ziel hierbei ist es, das Verhalten der Menschen zu ihrem Wohl bzw. zum Wohl der Gesellschaft zu beeinflussen. Dabei ist zu betonen, dass Personen selbst bestimmen können, ob sie die vorgegebene Richtung nachgehen oder ablehnen wollen (Thaler & Sunstein, 2020, 14 f.). Thaler und Sunstein (2020, S. 19) argumentieren, dass Nudging unter anderem die Vorsorge in der Gesundheit verbessern, Sparquoten steigern oder mehr Organspender werben könnte und ermutigen demnach private Institutionen, Behörden und Regierungen, Menschen bewusst zu guten Entscheidungen zu lenken (Thaler & Sunstein, 2020, S. 15). Nudging kann beispielsweise gesündere Essgewohnheiten hervorrufen. So untersuchten Hansen et al. (2016, S. 124) wie das Essverhalten bei Konferenzteilnehmer:innen durch die Anordnung von Kuchen und Obst beeinflusst werden kann. Sie konnten nachweisen, dass der Obstkonsum gesteigert und der Kuchenkonsum reduziert werden kann, wenn das Obst vor dem Kuchen präsentiert wurde (Hansen et al., 2016, S. 126).

3.1.2 Von Nudge zu Sludge

Was viele Forscher:innen nicht erwarteten, ist, in welchem Ausmaß das Konzept von Nudging für unmoralische Zwecke eingesetzt werden kann. So griffen vermehrt Unternehmen auf jene Techniken zurück, um ihren Profit zu steigern, wodurch oftmals Konsument:innen benachteiligt wurden (Narayanan et al., 2020, 72 f.). Dazu nahm Thaler

(2018, S. 431) Stellungnahme und trennt Nudge vom Missbrauch jener Techniken, welchen er als *Sludge* bezeichnet. Im Gegensatz zu Nudge, welcher die Absicht hat, Individuen zu guten Entscheidungen zu lenken, wird bei einem Sludge das Interesse des Individuums untergraben.

3.1.3 Einige Heuristiken und Urteilsfehler im Überblick

Hanson und Kysar (1999, S. 630) haben das Potenzial von Heuristiken und Urteilsfehlern erkannt, Konsument:innen gezielter anzusprechen, um damit den Profit von Firmen zu maximieren. Sie fassen dies unter dem Begriff *Markt Manipulation* zusammen. In ihrer Arbeit legen sie mehrere Arten von Verhaltensmustern offen, welche die Basis für die Markt Manipulation bilden. Diese umfassen unter anderem, Anker Effekte, Status-Quo-Vorurteile und Framing Effekte. Darüber hinaus gibt es weitere Urteilsverzerrungen und Heuristiken, von denen im Verkauf und Marketing, Gebrauch gemacht werden. Diese werden im Folgenden kurz vorgestellt.

3.1.3.1 Verankerungseffekt

Der Verankerungseffekt beschreibt, wie Menschen bei der Schätzung von unbekannten Größen auf Referenzwerte, sogenannte *Anker*, zurückgreifen, selbst wenn jene Referenzwerte eigentlich keine Relevanz für den Kontext haben (Tversky & Kahneman, 1974, S. 1128). Dementsprechend ergeben sich unterschiedliche Schätzwerte für unterschiedliche Ausgangswerte, die teils stark vom tatsächlichen Wert abweichen. Ein Beispiel innerhalb der Preisverhandlung veranschaulicht diesen Effekt: Der erste vorgeschlagene Preis für ein benutztes Auto wird zum Referenzpreis von weiteren Verhandlungen. Demnach scheinen Preise unter dem Referenzwert vernünftig zu sein, obwohl diese möglicherweise höher als der tatsächliche Wert des Autos sind (Harvard, 2023). Auch in Bereichen des Marketings und der Werbung kann der Verantwortungseffekt bewusst eingesetzt werden. Beispielsweise können unverbindliche Verkaufspreise (UVP) oder reduzierte Preise als Anker dienen und die Kaufbereitschaft der Kunden beeinflussen (Beck, 2014, S. 147).

3.1.3.2 Framing Effekt

Der Framing Effekt bezeichnet die Beobachtung, dass die Urteilsbildung von der Art und Weise wie Informationen präsentiert werden, abhängt. Folglich können zwei

verschiedene Formulierungen von einem Sachverhalt, mit identem Informationsgehalt, unterschiedlich interpretiert werden. Damit kann Framing das Entscheidungsergebnis beeinflussen (Beck, 2014, S. 153). Im Marketing wird häufig auf positives Framing zurückgegriffen (Spencer, 2020, S. 970). Ein solches Framing soll bewirken, ein Produkt oder eine Dienstleistung ansprechender zu gestalten. Beispielsweise kann ein Nahrungsmittel, welches anstatt mit „25% Fett“, mit „75% Mager“, gekennzeichnet ist, für Konsument:innen als gesünder empfunden werden. In der Tat konnten I. P. Levin und Gaeth (1988, S. 374) in einem Experiment zeigen, dass Konsument:innen zum „75% magerem“ Fleisch mehr tendierten als zum „25% fettigem“ Fleisch.

3.1.3.3 Status-quo-Bias und Default Effekt

Unter dem Status-quo-Bias wird die Tendenz, den bestehenden Zustand (Status quo) gegenüber Veränderungen zu bevorzugen, verstanden (Samuelson & Zeckhauser, 1988, S. 7). Diese kognitive Verzerrung ist häufig die Ursache dafür, dass ein Probeabonnement nicht zeitgerecht gekündigt wird (Thaler & Sunstein, 2020, S. 56). Verwandt mit dem Status-quo-Bias ist der Default Effekt. Dieser beschreibt, dass Menschen häufig Standardeinstellungen oder vorgewählte Optionen übernehmen (Johnson et al., 2002, S. 13). Eine Studie von Madrian und Shea (2001) untermauert diese Beobachtung. In ihrer Untersuchung kommen sie auf das Ergebnis, dass die Teilnehmeranzahl für die Altersvorsorge von 49% auf 86% erhöht werden kann, wenn die Einwilligung für die Teilnahme vorgewählt wird (Madrian & Shea, 2001, S. 1184).

3.1.3.4 Bandwagon Effekt

Der Bandwagon Effekt basiert auf dem menschlichen Bedürfnis nach Zugehörigkeit und sozialer Bestätigung. Sie beschreibt, dass Menschen dazu neigen ihre Vorlieben, die der Mehrheit anzugleichen. Folglich wird einem Produkt, welches von vielen Konsument:innen gekauft wird, ein höherer Stellenwert zugeschrieben (Bindra et al., 2022, S. 305).

3.1.3.5 Knappheitsheuristik

Verwandt mit dem Bandwagon Effekt ist die Knappheitsheuristik. Diese kognitive Verzerrung zeichnet sich dadurch aus, dass Konsument:innen knapp verfügbaren Produkten einen höheren Wert zuschreiben. Die Beobachtung wird damit erklärt, dass

Konsument:innen davon ausgehen, dass die Knappheit eines Produkts durch eine hohe Nachfrage entstanden ist. Dadurch schließen sie darauf, dass jene Produkte populär und hochwertig sein müssen (Herpen et al., 2005, S. 623).

3.1.3.6 Sunken-Costs-Fehlschuss

Der Sunken-Costs-Fehlschuss bezeichnet die Tendenz, Ressourcen in Form von Zeit, Geld oder Energie in eine Entscheidung, die sich als unrentabel erweist, weiterhin zu stecken. Betroffenen bereitet es Schwierigkeiten ihre Entscheidung zurückzuziehen, da sie bereits Investitionen getätigt haben (Haita-Falah, 2017, S. 44).

3.2 Täuschung und Manipulation im Handel

Narayanan et al. führen an, dass Dark Patterns zum Teil ihren Ursprung in manipulativen und täuschenden Praktiken, die im analogen Handel eingesetzt werden, haben. Unternehmen haben seit geraumer Zeit auf derartige Taktiken zurückgegriffen (Narayanan et al., 2020, S. 69). Im Folgenden werden einige davon kurz vorgestellt.

3.2.1 Schwellenpreis

Ein bekanntes Beispiel ist, den Preis von Produkten auf eine Zahl knapp unterhalb eines ganzzahligen Betrags zu setzen (Narayanan et al., 2020, 69 ff.). Jener Preis wird auch als *Schwellenpreis* oder *gebrochenen Preis* bezeichnet und ist in der heutigen Zeit gang und gäbe. So wird beispielsweise auf einem Preisschild statt „10 Euro“, „9,99 Euro“ angezeigt. In einer Studie konnten Bizer und Schindler (2005, S. 771) zeigen, dass diese Methode in der Tat effektiv ist, um den Umsatz zu steigern.

3.2.2 Werbebetrug

Werbebetrug ist eine weitere Strategie, die bereits mehrfach in der analogen Welt zum Einsatz gekommen ist, jedoch unter Umständen mit strengeren Konsequenzen verbunden ist. In solchen Fällen werden Konsument:innen falsche Fakten oder irreführende Informationen präsentiert (Nuseir, 2018, S. 454). Das Ziel dabei ist es, Produkte oder Dienstleistungen besser darzustellen, um Konsument:innen zum Kauf dieser zu bewegen. Beispielsweise wurde der Joghurt-Hersteller *Dannon* für die falsche Behauptung, dass *Activia* die „klinisch nachgewiesene“ Fähigkeit besitzt, die Verdauung

zu regulieren oder das Immunsystem durch probiotische Bakterien zu stärken, verklagt (Avila & Holding, 2009).

Weiters fanden Forscher:innen der Organisation *Consumers' Checkbook*, dass viele bekannte Händler:innen fälschlicherweise erhebliche Einsparungen beim Kauf von Aktionsartikeln, werben. Händler:innen setzen dabei den behaupteten Originalpreis für ein Produkt auf einen absurd hohen Wert, sodass der Preis nach einem hohen Rabatt dem tatsächlichen Wert entspricht. Anders ausgedrückt, handelt es sich dabei oft um den regulären Preis, der als ermäßigter Preis dargestellt wird (Brasler & Densmore, 2022).

3.2.3 Bait and Switch

Bait and Switch ist eine Praktik, die ebenfalls erwähnenswert ist. Diese verläuft in 3 Schritten: Zuerst legen Verkäufer:innen einen Köder, beispielsweise in Form einer Aktion aus, welcher als Kaufanreiz dient. Als nächstes hängen sich Konsument:innen im übertragenen Sinn an den Köder an und kontaktieren damit die Verkaufsperson. Im letzten Schritt weicht die Verkaufsperson von dem initial dargebotenen Angebot ab und wirbt ein teureres Produkt (Wilkie et al., 1998, S. 274). New Rapids Carpet Center, ist zum Beispiel ein Unternehmen, welches auf diese Methode zurückgriff. Dabei wurden Kund:innen mit dem Angebot angelockt, einen Teppichboden gratis zum Kauf eines Staubsaugers oder eines Teppichs zu erhalten. Sobald Kund:innen jedoch diese Aktion eingegangen sind, wurde ihnen mitgeteilt, dass der Teppichboden nicht mehr vorrätig sei (Wilkie et al., 1998, S. 273).

3.3 Growth Hacking

Narayanan et al. (2020, S. 74) argumentieren, dass Dark Patterns ihren direkten Ursprung im *Growth Hacking* haben. Growth Hacking bezeichnet eine Marketingstrategie, die darauf abzielt, mit wenigen Ressourcen die Nutzerzahl eines Produkts zu steigern. Die Strategie etablierte sich, nachdem Startups oftmals über kein ausreichendes Budget oder Expertise für herkömmliche Werbung verfügten. Somit waren viele von ihnen auf ressourcenärmere Marketingpraktiken angewiesen und entwickelten eigene kreative Methoden, die sich oftmals sogar als effektiver erwiesen als herkömmliches Marketing (Holiday, 2012). Dabei zogen sie Erkenntnisse aus den Bereichen Design,

Programmierung und Marketing und entwickelten bisher unbekannte Techniken, um die Produktakzeptanz und die Bekanntheit zu fördern.

Ein bekanntes Beispiel ist, wie Hotmail seine Anwendergruppe ausweitete. Hotmail ging dabei folgendermaßen vor: Jede E-Mail, die von einem seiner Nutzer:innen verschickt wurde, enthielt auf der Unterseite eine E-Mail-Signatur mit der Aufschrift „*Get your free email with Hotmail*“. Damit warben Nutzer:innen für Hotmail und sorgten für ein explosionsartiges Wachstum (Narayanan et al., 2020, S. 74).

3.3.1 Zwei Werkzeuge: Nudging und A/B-Testing

Nach Narayanan et al. (2020, S. 75) verhelfen zwei Werkzeuge Growth Hackers bei der Entwicklung von effektiven Marketingtechniken. Auf der einen Seite bieten Erkenntnisse aus der Nudge-Bewegung Einsicht in die Verhaltensmustern der Individuen. Auf der anderen Seite können mittels A/B-Tests Benutzeroberflächen effizient optimiert werden. Hierbei werden beispielsweise zwei Varianten von einer Benutzeroberfläche, die sich nur minimal in ihrem Design unterscheiden, gegenübergestellt. Diese werden an zwei oder mehreren Benutzergruppen getestet, um Unterschiede im Verhalten zu identifizieren, die durch bestimmte Designelemente ausgelöst werden. Basierend auf den daraus resultierenden Ergebnissen, kann festgestellt werden welches der beiden Varianten besser geeignet ist (Narayanan et al., 2020, 75 f.).

3.3.2 Manipulierendes und irreführendes Growth Hacking

Growth Hacking hat auch seine Schattenseiten. So wurde Growth Hacking in der Praxis ebenfalls dafür verwendet, Benutzer:innen zu überlisten, um damit den Profit eines Unternehmens zu steigern (Narayanan et al., 2020, S. 75). Einige Fälle führten sogar zu rechtlichen Konsequenzen. Ein Beispiel hierfür ist die soziale Medienplattform LinkedIn, welches durch irreführendes Design Zugriff auf die Kontakte von Nutzer:innen erlangte und ohne deren Wissen Einladungen an diese verschickte. Dem Unternehmen wurde schließlich eine Strafe von 13 Millionen Dollar verhängt (Strange, 2015). Mit dem Einsatz von Growth Hacking für unethische Zwecke kristallisierten sich allmählich Dark Patterns heraus (Narayanan et al., 2020, S. 75).

4 Arten von Dark Patterns

Das vorliegende Kapitel verfolgt das Ziel, einen Überblick über verschiedene Arten von Dark Patterns zu verschaffen. Zunächst werden verschiedene Typologien angeführt, wobei betont wird, dass es schwierig ist, eine umfassende Typologie zu erstellen. Anschließend wird eine erweiterte Typologie von Gray et al. (2018), die die Kategorien *Nagging*, *Obstruction*, *Sneaking*, *Interface Interference*, *Forced Action*, *Social Proof* und *Urgency* umfasst, nähergebracht. Im Zuge dessen werden Beispiele für Dark Patterns aus jeder dieser Kategorien gezeigt.

4.1 Verschiedene Typologien von Dark Patterns

Angesichts der zunehmenden Vielfalt an Dark Patterns und der daraus resultierenden Komplexität ist es nötig, diese auf eine übersichtlichere Art und Weise zu organisieren. Infolgedessen beschäftigten sich mehrere Forscher:innen mit der Kategorisierung von Dark Patterns und sammelten gleichzeitig zahlreiche Beispiele dafür (Organisation für wirtschaftliche Zusammenarbeit und Entwicklung [OECD], 2022, S. 10).

Conti und Sobiesk (2010, S. 272) sind eine der ersten Forscher:innen, die erstmals von *bösartigem Interfacedesign* sprachen und stellen in ihrer Arbeit eine Klassifizierung von jenem bereit. Sie identifizierten 11 Hauptkategorien: *Coercion*, *Confusion*, *Distraction*, *Exploiting Errors*, *Forced Work*, *Manipulating Navigation*, *Obfuscation*, *Restricting Functionality*, *Shock* und *Trick* (Conti & Sobiesk, 2010, S. 272). Bösch et al. (2016, S. 239) nehmen sich in ihrer Arbeit Täuschungspraktiken im Bereich der Privatsphäre vor und stellen sogenannte *Privacy Dark Strategies* vor, mit derer Hilfe Dark Patterns nach ihrem Zweck klassifiziert werden können. Ebenso führt der Europäische Datenschutzausschuss (EDSA) eine Klassifizierung von Dark Patterns, die bezüglich des Datenschutzes relevant sind, ein. Aus dieser gehen die Kategorien *Overloading*, *Skipping*, *Stirring*, *Obstructing*, *Fickle* und *Left in the dark*, hervor (Europäischer Datenschutzausschuss [EDSA], 2023, 65 ff.). Mathur et al. (2019, S. 5) fokussieren sich darauf, wie sich Dark Patterns auf Benutzer:innen auswirken und kategorisieren diese entsprechend. Sie unterscheiden die Kategorien *Asymmetric*, *Covert*, *Deceptive*, *Hides Information* und *Restrictive* (Mathur et al., 2019, S. 5). Gray et al. (2018, S. 4) streben eine generische Typologie an. Dabei baut ihre Typologie auf den von Brignull (2010) erarbeiteten Arten von Dark Patterns auf: *Bait and Switch*, *Disguised Ad*,

Forced Continuity, *Friend Spam*, *Hidden Costs*, *Misdirection*, *Price Comparison Prevention*, *Privacy Zuckering*, *Roach Motel*, *Sneak into Basket* und *Trick Questions*. Gray et al. (2018, S. 4) ergänzen diese Sammlung um weitere Dark Patterns und unterteilen diese in fünf grobe Kategorien: *Nagging*, *Obstruction*, *Sneaking*, *Interface Interference* und *Forced Action* (Abbildung 1).

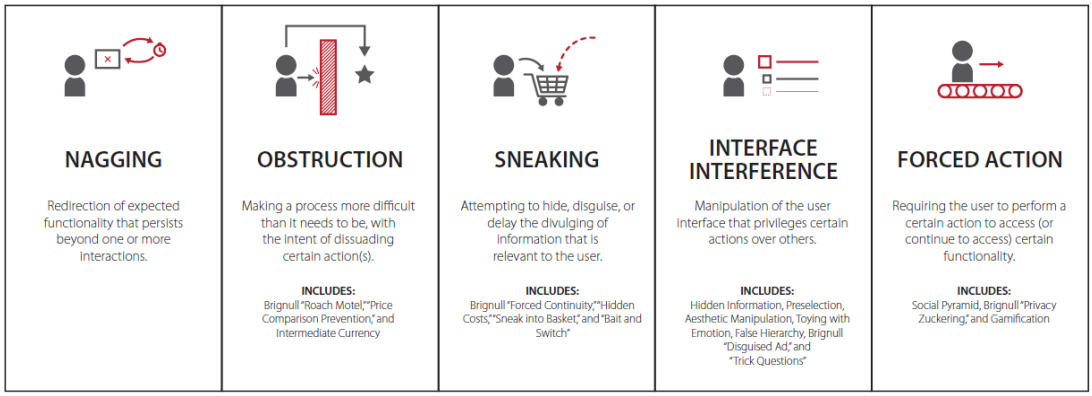

Abbildung 1: Dark Pattern Strategien von Gray et al. (Gray et al., 2018, S. 5)

4.2 Keine allumfassende Typologie

Die Wahrscheinlichkeit, dass zu einem späteren Zeitpunkt eine endgültige Klassifikation für alle Dark Patterns vorliegt, ist aus mehreren Gründen gering. Zum einen ist es absehbar, dass durch den Fortschritt von Technologien und die Entwicklung neuer Formen von Benutzeroberflächen kontinuierlich neue Dark Patterns entstehen werden. Somit können gegenwärtige Typologien nicht garantieren, zukünftige Dark Patterns miteinzuschließen. Zum anderen passen sich Typologien den Forschungszielen der Forscher:innen an. Da Autor:innen Grenzen für ihre Arbeit setzen müssen, ist es unausweichlich, dass einige Praktiken unberücksichtigt bleiben. Beispielsweise legen Mathur et al. (2019) den Fokus ausschließlich auf Instanzen, die mit Web-Crawling ausfindig gemacht werden können. Damit enthält ihr Datensatz überwiegend textbasierte anstelle von designbasierten Dark Patterns. Andere Typologien beruhen auf spezifischen Kontexten wie Datenschutz und Privatsphäre (OECD, 2022, S. 11). Hier gelten die Typologien von dem EDSA (2023) oder von Bösch et al. (2016) als Beispiele.

4.3 Erweiterte Typologie von Gray et al.

Nachfolgend wird eine erweiterte Typologie von Gray et al. (2018) erläutert, welche die gängigsten Dark Patterns, die in der Literatur genannt werden, abdeckt. Diese umfasst die Kategorien *Nagging*, *Obstruction*, *Sneaking*, *Interface Interference*, *Forced Action*, *Urgency* und *Social Proof*. Dennoch ist anzumerken, dass diese Typologie unvollständig ist.

4.3.1 Nagging

Dark Patterns, die der Kategorie *Nagging* zugeordnet sind, stören so lange den Interaktionsfluss der Nutzer:innen, bis sie eine Aktion tätigen, die im Interesse der Anbieter:innen liegen. Häufig geschieht dies durch wiederkehrende Pop-ups, die beispielsweise darauf abzielen, Nutzer:innen zur Aktivierung der Benachrichtigung oder der Standortverfolgung zu überreden. Ein solches Dark Pattern ist in Abbildung 2 zu sehen. Um das Pop-up zu schließen, stehen die Optionen "OK" oder "Not Now" zur Auswahl. Solange „OK“ nicht getätigt wird, wird das Pop-up zu einem späteren Zeitpunkt erneut angezeigt (Gray et al., 2018, S. 5).

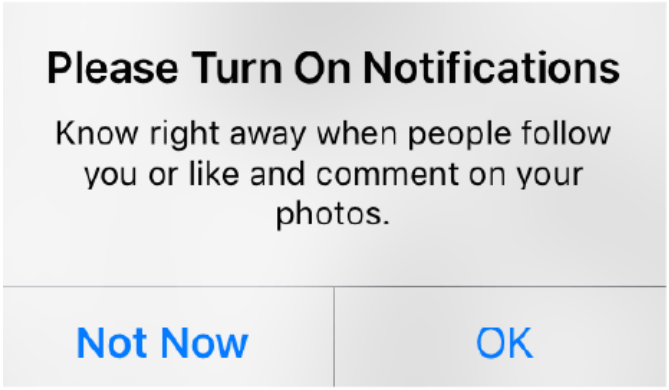

Abbildung 2: Ein Beispiel für *Nagging* (Gray et al., 2018, S. 5)

4.3.2 Obstruction

Unter *Obstruction* fallen Dark Patterns, die es Nutzer:innen erschweren, ein bestimmtes Ziel zu erreichen. Dabei werden Interaktionsabläufe mit Absicht komplex gestaltet, um Nutzer:innen von bestimmten Aktionen abzuhalten (Gray et al., 2018, S. 5). Ein typisches Dark Pattern hierfür ist das sogenannte *Roach Motel*, welches in der Literatur ebenfalls unter dem Namen *Hard to Cancel* bekannt ist (Europäische Kommission

[EK] et al., 2022, S. 31). Diese zeichnen sich durch Situationen aus, die einfach zu betreten, jedoch schwer zu entkommen sind. Ein Beispiel hierfür ist, dass die Registrierung für eine Dienstleistung reibungslos verläuft, jedoch die Kündigung dieser auf große Hindernisse stößt. *Price Comparison Prevention* ist ein weiteres Dark Pattern, welches *Obstruction* zugeordnet wird. Wie der Name suggeriert, verhindert dieses Dark Pattern den Preisvergleich von Produkten. Ein Beispiel, in dem dieses realisiert wird, ist, mittels JavaScript das Markieren von Texten auf Webseiten zu deaktivieren, wodurch Besucher:innen verhindert wird, Produktnamen zu kopieren und damit das Recherchieren nach demselben Produkt zu einem niedrigeren Preis, erschwert wird. Ein weiteres Dark Pattern der Kategorie *Obstruction* ist *Intermediate Currency*. Hierbei handelt es sich um den Einsatz einer virtuellen Währung. Damit wird es Nutzer:innen erschwert, den tatsächlichen Wert eines Produkts oder einer Dienstleistung nachzuvollziehen. (Gray et al., 2018, S. 6).

4.3.3 Sneaking

Sneaking umfasst Dark Patterns, die relevante Informationen verstecken oder verspätet anzeigen. Darunter fallen Dark Patterns wie *Forced Continuity*, *Hidden Costs*, *Sneak into Basket* und *Bait and Switch* (Gray et al., 2018, S. 6). *Forced Continuity*, auch bekannt als *Hidden Subscription* (EK et al., 2022, S. 30), bezeichnet Designmuster, die automatisch Abonnements verlängern, wodurch oftmals unbemerkt Kosten für Konsument:innen verrechnet werden. Dieses Dark Pattern macht sich die durch Konsument:innen vernachlässigte Überprüfung der Kündigungsfrist zu Nutze. Das Dark Pattern *Hidden Costs* deutet auf Instanzen, bei welchen hohe Zusatzkosten zu Beginn verborgen werden und erst kurz vor dem Zahlungsvorgang bekannt gegeben werden (Gray et al., 2018, S. 6). *Sneak into Basket* beschreibt eine Vorgehensweise, bei der Produkte ohne die Einwilligung der Konsument:innen in den Warenkorb hinzugefügt werden, in der Erwartung, dass diese von Konsument:innen gekauft werden. Oftmals sind jene Produkte Empfehlungen basierend auf den von Konsument:innen ausgewählten Produkten (Gray et al., 2018, S. 6). Designmuster, welche den Angebotscharakter von User-Interface-Elementen für Täuschungen ausnutzen, fasst Brignull (2010) in *Bait and Switch* zusammen. Beispielsweise nutzte Microsoft diese Praktik, um Nutzer:innen zu überreden ihre Systeme auf Windows 10 zu aktualisieren. Dabei ging Microsoft so weit, die Bedeutung vom „X“ Knopf auf der rechten oberen Ecke umzukehren, sodass die Auswahl dieses Knopfs die Aktualisierung startet (Brignull, 2010).

4.3.4 Interface Interference

Die Kategorie Interface Interference umfasst Dark Patterns, die bestimmten Aktionen deutlichen Vorrang gegenüber anderen geben. Es werden dabei drei Unterkategorien unterschieden: *Hidden Information*, *Preselection* und *Aesthetic Manipulation* (Gray et al., 2018, S. 7).

4.3.4.1 Hidden Information

Das Dark Pattern *Hidden Information* verschweigt Informationen und Aktionen, die für Nutzer:innen relevant sind und kennzeichnet diese absichtlich als irrelevant. Bewerkstelligt wird dies beispielsweise mit dem Einsatz von kleingedruckter Schrift, schlecht sichtbaren Farben sowie das Verstecken von Optionen. In Abbildung 3 ist beispielsweise die Option, die es erlaubt Werbematerial an die E-Mail-Adresse zu schicken, unter „More info“ versteckt (Gray et al., 2018, S. 7).

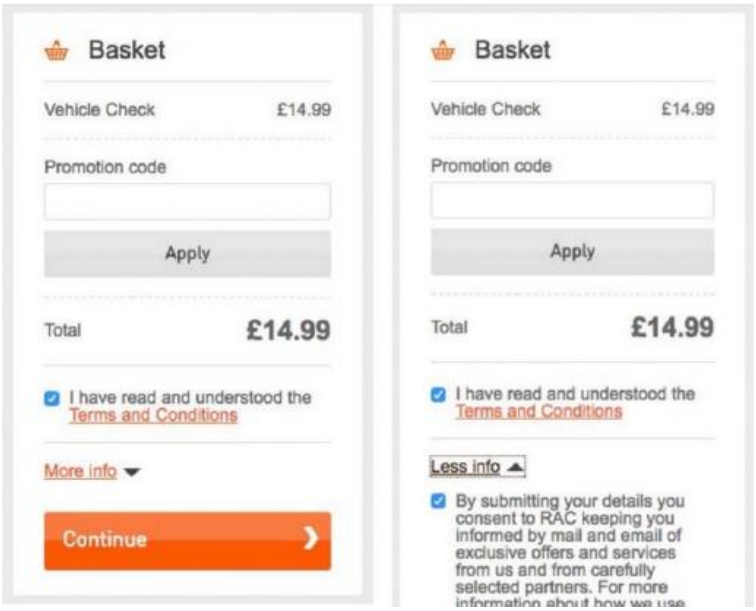

Abbildung 3: Ein Beispiel für *Hidden Information* und *Preselection* (Gray et al., 2018, S. 7)

4.3.4.2 Preselection

Das Dark Pattern *Preselection* repräsentiert Instanzen, bei welchen Optionen, die von Anbieter:innen bevorzugt werden, vorausgewählt sind (Gray et al., 2018, S. 7). Abbildung 3 veranschaulicht ebenfalls dieses Dark Pattern.

4.3.4.3 Aesthetic Manipulation

Die Kategorie *Aesthetic Manipulation* fokussiert sich mehr auf die Darstellung als auf die Funktion von User Interface (UI) Elementen. *Aesthetic Manipulation* umfasst die Dark Patterns wie *Toying with Emotion*, *False Hierarchy*, *Disguised Ad* und *Trick Questions* (Gray et al., 2018, S. 7). *Toying with Emotion* beschreibt Designmuster, die mithilfe von emotionalem Text und visuellen Elementen Sachverhalte framen und damit unangenehme Emotionen, wie Schuldgefühle und Scham, in Nutzer:innen auslösen. (Gray et al., 2018, S. 7). In diesem Zusammenhang sprechen Forscher:innen auch häufig von *Confirmshaming* (Brignull, 2010; EK et al., 2022, S. 30). Abbildung 4 veranschaulicht ein Beispiel von dem soeben vorgestellten Dark Pattern. Mit der abwertenden Beschreibung „no, I prefer to bleed to death“, wird versucht, Nutzer:innen zu überzeugen die Benachrichtigungen zu aktivieren.

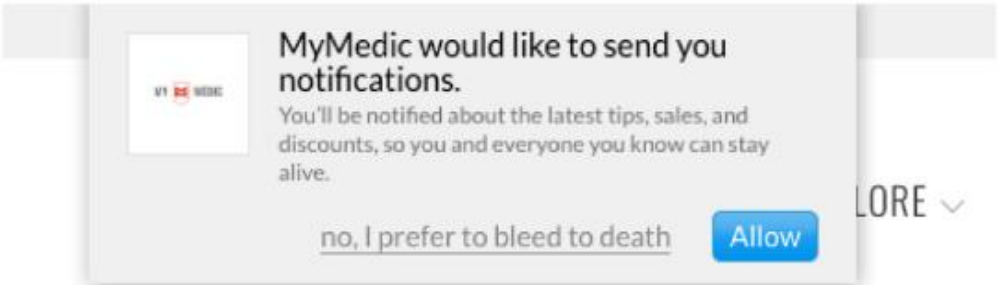

Abbildung 4: Ein Beispiel für *Confirmshaming* (Brignull, 2010)

Unter *False Hierarchy* werden Designmuster verstanden, die bestimmten Optionen Vorrang gegenüber anderen geben. Optionen, die Nutzer:innen nicht wählen sollten, werden bewusst in den Hintergrund gerückt. So soll erreicht werden, dass Nutzer:innen sich für die von Anbieter:innen bevorzugte Option entscheiden (Gray et al., 2018, S. 7). Ein Beispiel ist in Abbildung 5 dargestellt. Die nicht präferierte Option ist ausgegraut, wodurch der Eindruck vermittelt wird, dass jene Option deaktiviert ist und damit nicht ausgewählt werden kann (Mathur et al., 2019).

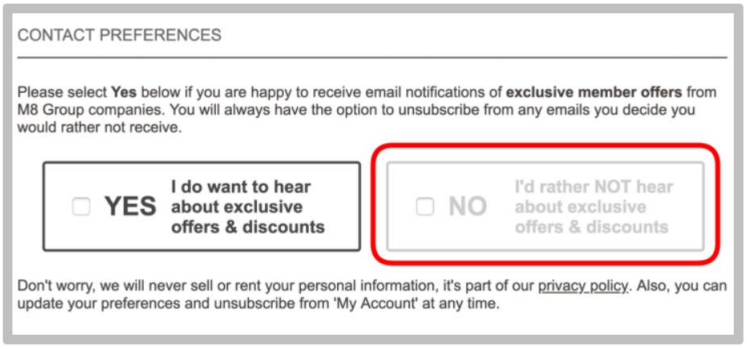

Abbildung 5: Ein Beispiel für False Hierarchy (Mathur et al., 2019)

Das Dark Pattern *Disguised Ad* bezeichnet Werbeanzeigen, die nicht als solche zu erkennen sind und für Nutzer:innen als integralen Bestandteil der Benutzeroberfläche wahrgenommen werden. Diese können beispielsweise als interaktive Spiele oder Download-Tasten getarnt sein. Sobald Nutzer:innen auf jenen Bereich klicken, werden sie zu einer anderen Seite navigiert, anstatt, dass die zu erwartende Funktion ausgeführt wird (Gray et al., 2018, S. 7). Beim Dark Pattern *Trick Questions* handelt es sich um Fragen und Beschreibungen, die besonders komplex formuliert sind, um Nutzer:innen zu überlisten. Hierfür greifen Designer:innen beispielsweise auf Doppelnegationen sowie den Tausch der Bedeutung von „Opt-in“ und „Opt-out“ bei Checkboxen zurück (Gray et al., 2018, S. 8). Abbildung 6 zeigt, wie dieses Dark Pattern im Registrierungsprozess umgesetzt wurde. In diesem Beispiel ist die Bedeutung der beiden Optionen entgegengesetzt: Das Anklicken der ersten Option führt dazu, dass ihr nicht zugestimmt wird, während die Wahl der zweiten Option das Gegenteil bewirkt (Brignull, 2010).

Abbildung 6: Ein Beispiel für *Trick Questions* (Brignull, 2010)

4.3.5 Forced Action

Dark Patterns der Kategorie *Forced Action* zwingen Nutzer:innen eine bestimmte Aktion durchzuführen, um Zugriff auf eine Dienstleistung zu erhalten (Gray et al., 2018, S. 8). Das Dark Pattern *Social Pyramid* verfolgt das Ziel, die Anwendergruppe einer

Dienstleistung durch Kontakte der Nutzer:innen auszuweiten. Dazu werden Nutzer:innen beispielsweise aufgefordert ihre Freund:innen einzuladen, um bestimmte Features freigeschaltet zu bekommen. *Privacy Zuckering* ist ein weiteres Dark Pattern, welches unter *Forced Action* fällt. Dieses zwingt Nutzer:innen mehr Daten über sich selbst bekannt zu geben, als sie es vorgehabt hätten. Eine übliche Vorgehensweise ist es, mehrere Einwilligungserklärungen zu kombinieren. So könnten beispielsweise Einwilligungserklärungen für den Verkauf von Daten an Dritte in Geschäftsbedingungen versteckt werden (Gray et al., 2018, S. 8). Abbildung 7 zeigt ein weiteres Beispiel: Mit der Tätigung des verpflichtenden Checkboxes zur Bestätigung der Geschäftsbedingungen geht die Einwilligung, Werbungen zu erhalten, einher. Durch den Einsatz vom Dark Pattern *Gamification* werden Nutzer:innen bestimmte Dienstleistungen ohne Geldausgabe schwer zugänglich gemacht. Dies betrifft oftmals Spiele, in welchen die nächsthöheren Levels zunehmend schwerer zu erreichen sind, sodass Nutzer:innen gezwungenermaßen gegen Entgelt auf Powerups oder Extraleben zurückgreifen müssen (Gray et al., 2018, S. 8). *Forced Registration* ist ebenfalls ein Dark Pattern, welches *Forced Action* zugeordnet wird. Dabei werden Nutzer:innen gezwungen ein Konto zu erstellen oder überlistet, dies für notwendig zu halten (EK et al., 2022, S. 30).

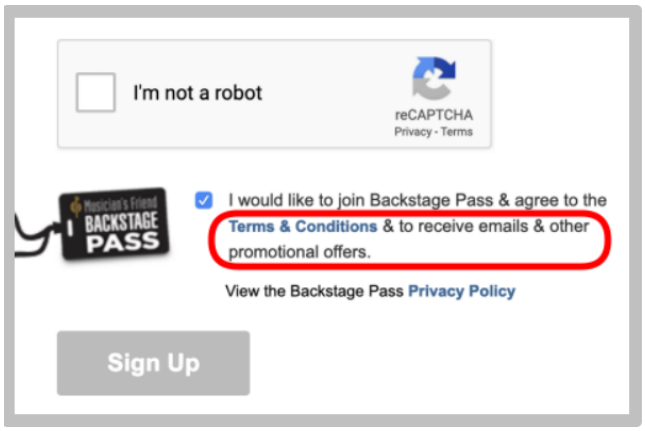

Abbildung 7: Ein Beispiel für *Forced Action* (Mathur et al., 2019)

4.3.6 Social Proof

Dark Patterns der Kategorie *Social Proof* nutzen primär den Bandwagon Effekt (siehe 3.1.3.4) aus. In anderen Worten beruhen sie auf das menschliche Bedürfnis nach sozialer Bestätigung und dem Vertrauen in die Entscheidung anderer. Sie versuchen, Nutzer:innen zu einer Handlung zu verleiten, indem vorgetäuscht wird, dass viele

andere Menschen derselben Handlung nachgehen. Dark Patterns wie *Activity Message* und *Testimonials* werden dieser Kategorie zugeordnet. Dabei bezieht sich *Activity Message* auf irreführende Mitteilungen über die Aktivitäten anderer Konsument:innen, während *Testimonials* falsche Bewertungen von Konsument:innen beschreiben (Mathur et al., 2019, S. 12).

4.3.7 Urgency

Dark Patterns der Kategorie *Urgency* vermitteln Nutzer:innen ein Gefühl der Dringlichkeit und verleiten sie damit zu einer schnellen Handlung (OECD, 2022, S. 11). Mit den Dark Patterns *Low Stock Message* oder *High Demand Message* werden Konsument:innen fälschlicherweise auf eine Warenknappheit bzw. auf eine hohe Nachfrage hingewiesen (Mathur et al., 2019, 20 f.). In Abbildung 8 ist ein Beispiel von *Low Stock Message* ersichtlich. Weitere Dark Patterns dieser Kategorie sind *Countdown Timer* und *Limited Time Message*, welche suggerieren, dass ein Angebot oder eine Aktion in Kürze abläuft. Ersteres handelt vom Einsatz von Count-Down Uhren, wie beispielsweise in Abbildung 9 zu sehen ist. Diese Count-Down Uhren setzen sich in vielen Fällen wieder zurück. Darüber hinaus gibt es Fälle, in denen die Count-Down Uhren zwar ablaufen, jedoch das Angebot weiterhin angezeigt wird. *Limited Time Message* vermittelt mit einer Nachricht den Auslauf einer Aktion, kündigt jedoch die genaue zeitliche Frist nicht an (Mathur et al., 2019, S. 15). Ein Beispiel für *Limited Time Message* ist in Abbildung 10 vorzufinden.

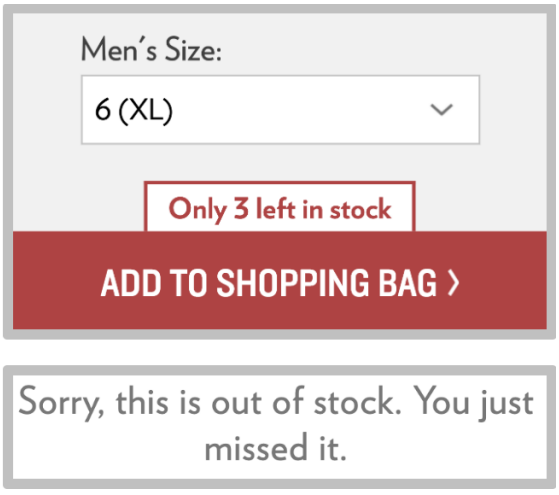

Abbildung 8: Ein Beispiel für *Countdown Timer (Mathur et al., 2019)*

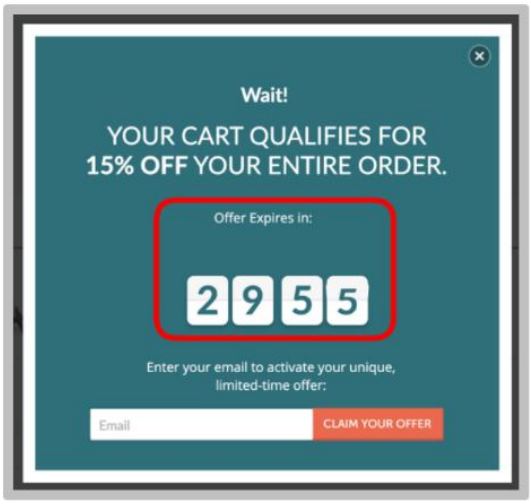

Abbildung 9: Ein Beispiel für *Low Stock Message* (Mathur et al., 2019)

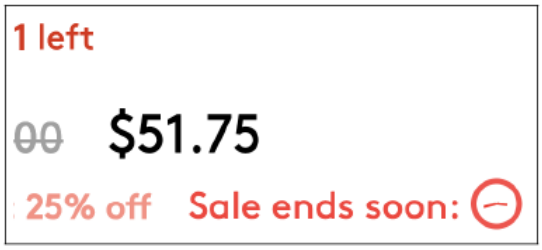

Abbildung 10: Ein Beispiel für *Limited Time Message* (Mathur et al., 2019)

4.4 Überschneidungen von Dark Patterns in verschiedenen Kategorien

Es ist anzumerken, dass Dark Patterns in mehrere der zuvor genannten Kategorien eingestuft werden können. Beispielsweise könnte das in Abbildung 3 veranschaulichte Dark Pattern aus *Interface Interference*, ebenfalls *Sneaking* zugeordnet werden, da die zweite Option versteckt wird. Darüber hinaus könnte *Low Stock Message* und *High Demand Message* ebenfalls unter *Social Proof* fallen, da die Warenknappheit eine soziale Bestätigung implizieren kann (siehe 3.1.3.5).

5 Auswirkungen von Dark Patterns

Unternehmen nutzen Dark Patterns, um ihren Umsatz zu steigern. Narayanan et al. (2020, S. 77) führen an, dass dafür drei Ressourcen aus Konsument:innen geschöpft werden: Geld, Daten und Aufmerksamkeit. Demnach schaffen einige Dark Patterns Kaufanreize, sodass Konsument:innen mehr Geld ausgeben, als sie es sonst getan hätten. Andere Dark Patterns verleiten Konsument:innen dazu, ihre persönlichen Daten preiszugeben. Weiters gibt es Dark Patterns, die die Aufmerksamkeit der Nutzer:innen zu sich ziehen und ein Suchtverhalten auslösen können. Alles in allem läuft es darauf hinaus, dass die Autonomie der Betroffenen eingeschränkt wird (Narayanan et al., 2020, S. 77). Im Folgenden werden Auswirkungen von Dark Patterns in Bezug auf Geld, Daten und Aufmerksamkeit angeführt. Mit ausgewählten Instanzen von Dark Patterns wird veranschaulicht, wie Dark Patterns es ermöglichen jene herbeizuführen.

5.1 Finanzieller Schaden

Eine Gefahr, der Konsument:innen ausgesetzt sind, ist die des Geldverlusts. Eine Reihe von Dark Patterns überzeugt unterschwellig Konsument:innen mehr Geld auszugeben, als sie ursprünglich geplant hatten. Sie überreden Konsument:innen dazu Produkte oder Dienstleistungen zu kaufen, die sie sonst nicht oder in einer kleineren Menge erworben hätten (Narayanan et al., 2020, S. 77).

Dark Patterns können die Kaufbereitschaft bei Kund:innen erhöhen, indem sie bestimmte Emotionen bei ihnen auslösen. So werden im Bereich des E-Commerce häufig der Bandwagon Effekt (siehe 3.1.3.4) und die Knappheitsheuristik (siehe 3.1.3.5) ausgenutzt. Bei einigen Produkten wird beispielsweise angezeigt, dass andere Personen ebenfalls vor derselben Kaufentscheidung stehen (*Activity Message*). Damit wird ein sozialer Druck ausgeübt, wodurch Konsument:innen dazu verleitet werden sollen, das Produkt ebenfalls zu erwerben. Eine solche Information könnte beispielsweise lauten: „14 andere Personen sehen sich diesen Artikel gerade an“. Weiters wird durch das Anzeigen von gekauften oder unechten Rezensionen, sogenannte *Testimonials*, das Ziel verfolgt, ein Produkt als hochwertig, vertrauensvoll und gefragt einzustufen (Arbeiterkammer [AK], 2023, S. 12). Dark Patterns Instanzen, die auf Warenknappheit hinweisen, haben eine ähnliche Intention. Informationen wie „Nur noch 2 auf Lager“ (*Low Stock/ High Demand Message*) lösen nicht nur einen zeitlichen Druck aus,

sondern erwecken ebenfalls den Anschein, dass es sich um ein gutes Produkt handeln muss. Daraus resultiert ein Drang bei Konsument:innen, den Kauf unverzüglich zu tätigen, ohne über die Kaufentscheidung ein zweites Mal nachzudenken. Womöglich hätten sich die Konsument:innen nach einer Reflexion gegen ihre impulsive Entscheidung gerichtet (AK, 2023, S. 15).

Eine weitere Art den Kaufimpuls zu erhöhen, liegt in der Kosten- und Preisgestaltung. So legen bestimmte Onlineservices eine virtuelle Währung (*Intermediate Currency*) fest, um Konsument:innen die tatsächlichen Kosten weitgehend vorzuenthalten oder den Preisvergleich zu erschweren. Onlineservices nutzen zudem die Strategie, hohe Zusatzkosten (*Hidden Costs*) in Form von beispielsweise Versandkosten oder Servicepauschalen erst gegen Ende des Bezahlvorgangs zu offenbaren. Zum einen wirken separate Kosten attraktiv auf die Produkt-Preise. Zum anderen steigt durch die späte Offenlegung dieser Kosten die Wahrscheinlichkeit, dass Konsument:innen den Kauf abschließen, da sie bereits viel Zeit investiert haben, die Produkte zu finden. Dahinter steckt der Sunken-Costs-Fehlschuss (siehe 3.1.3.6). Weiters können Lockvogel-Angebote (*Bait and Switch*) die Preise im ersten Moment attraktiver gestalten. Beispielsweise implementiert der Onlineshop Eis.at diese Strategie. Auf jener Produktseite werden gelegentlich kostenlose Produkte angezeigt. Sobald ein solches Produkt ausgewählt wird, wird jedoch an der Kassa eine Mindestbestellung verlangt (AK, 2023, 12 f.).

5.2 Gefährdung der Privatsphäre

Dark Patterns zielen nicht nur darauf ab Geld zu generieren, sondern auch an die Daten der Nutzer:innen zu gelangen. Damit steht ebenso die Privatsphäre der Nutzer:innen auf dem Spiel (Narayanan et al., 2020, S. 77).

5.2.1 Die Wichtigkeit Daten zu schützen

Die Bewahrung der Privatsphäre im Internet ist aus vielzähligen Gründen von Bedeutung. Wenn persönliche Daten in die falschen Hände gelangen, können erhebliche Schäden für Betroffene entstehen. Diese umfassen Identitätsdiebstahl (Kahn & Roberds, 2008), Diskriminierung (Favaretto et al., 2019), Manipulationen (Susser et al., 2019) sowie Phishing Attacken (Shankar et al., 2019), um nur einige zu nennen. So besteht die Sorge, dass persönliche Daten an sogenannte *Data Brokers* übermittelt

werden. Data Brokers sind Unternehmen, die enorme Mengen an Daten sammeln, diese verarbeiten, um sie schließlich anderen Unternehmen gegen Entgelt weiterzuleiten. Die Daten, die dabei erworben werden, schließen unter anderem demografische, wirtschaftliche, gesundheitliche und verhaltensbasierte Informationen ein (Crain, 2018, S. 90). Die oben erwähnten Schäden werden durch Data Brokers verschärft. Nach Ankauf können Unternehmen mittels dieser Daten unter anderem Nutzer:innen manipulieren. Wie viel Macht Daten haben können, zeigt der Skandal von Cambridge Analytica. Dabei wurden Millionen von Datensätzen gesammelt, darunter viele aus Facebook Profilen, um politische Wahlen zu beeinflussen (Cadwalladr & Graham-Harrison, 2018). Ein anderes Beispiel ist, wie Facebook Werbetreibenden die Möglichkeit gab, basierend auf seinen umfangreichen Daten zur psychischen Verfassung von Teenagern gezielt Werbung an labile Teenager auszuspielen (S. Levin, 2017).

5.2.2 Datenschutzfeindliche Dark Patterns

Eine Vielzahl von Dark Patterns zielt darauf ab die Zustimmung der Nutzer:innen zur Sammlung und Verarbeitung ihrer Daten zu erlangen. Mit *Nagging* kann erreicht werden, dass Nutzer:innen mehr persönliche Daten hergeben als für den Zweck der Verarbeitung erforderlich. Dabei werden Nutzer:innen beispielsweise mit einem Pop-up-Fenster wiederholt aufgefordert bestimmte Daten nachzutragen oder bestimmten Verarbeitungszwecken zuzustimmen. Dies wird so lange praktiziert, bis Nutzer:innen letztendlich nachgeben (EDSA, 2023, S. 17). Eine weitere Möglichkeit ist es, Nutzer:innen es schwer zu machen, sich durch die Datenschutzinformationen zu navigieren, sodass sie bestimmte Informationen oder Kontrollmechanismen nicht ausfindig machen können. Dies wird bezeichnet als *Privacy Maze*. Eine Webseite, die in ihren Datenschutzbestimmungen angibt, dass ein bestimmtes Dokument weiterführende Informationen zu Datenschutzregelungen enthält, jedoch keinen Link zu jenem Dokument anführt und stattdessen auf den Q&A Abschnitt verweist, ist ein Beispiel hierfür (EDSA, 2023, 30 f.). Optionen, die die Sammlung und Verarbeitung der Daten erlauben, vorauszuwählen (*Preselection*), stellt sich ebenfalls als effektiv dar. Dies lässt sich durch den *Default Effekt* ergründen (siehe 3.1.3.3). Darüber hinaus können Nutzer:innen mittels inkonsistenten Interfaces in die Irre geführt werden. Wenn ein Designmuster, an welches sich Nutzer:innen gewöhnt haben, verändert wird, kann es zur unwillentlichen Vergabe der persönlichen Daten führen (EDSA, 2023, S. 69). Hier dient die Abwechslung zwischen Opt-in und Opt-out als Beispiel (*Trick Question*).

5.3 Beeinflussung der Aufmerksamkeit

Ein weiteres Ziel von Dark Patterns besteht darin, die Aufmerksamkeit der Nutzer:innen zu gewinnen, um dadurch die verbrachte Zeit mit den Anwendungen zu maximieren. Dies kann wiederum dazu führen, dass mehr Geld generiert und mehr Daten erlangt werden (Narayanan et al., 2020, S. 77). Das Unternehmen Uber setzt beispielsweise gamifizierte Elemente ein, um Fahrer:innen zu längeren Arbeitsschichten zu bewegen. Sobald Fahrer:innen sich entscheiden ihren Arbeitstag zu beenden, erscheint ein Pop-up Fenster mit der Nachricht, dass Fahrer:innen kurz davor stehen das Tagesziel für ein Einkommen zu erreichen. Mit der Tendenz, dass Personen sich ein bestimmtes Einkommen als Ziel festlegen, erhöht sich die Wahrscheinlichkeit, dass Fahrer:innen ihre Arbeit fortsetzen (Gray et al., 2018, S. 5).

5.3.1 Auslösen eines Suchtverhaltens

Die Beeinflussung der Aufmerksamkeit durch Dark Patterns kann zu einem Suchtverhalten führen. In solchen Fällen kann die Kontrolle über die Nutzung der Anwendungen verloren gehen. Gleichzeitig können Betroffene von ihrem Vorhaben abgelenkt werden, das Zeitgefühl verlieren und ein Bedauern nach der Interaktion verspüren (Monge Roffarello & Russis, 2022, S. 2). Lukoff et al. (2021) sprechen in diesem Zusammenhang erstmals von sogenannten *attention-capture Dark Patterns*. Diese gehen über die klassischen Dark Patterns hinaus, da sie nicht nur auf UI-Elemente beschränkt sind, sondern ebenfalls Systemfunktionen wie *Autoplay* oder *Pull-to-Refresh*, miteinbeziehen (Monge Roffarello & Russis, 2022, S. 1). *Autoplay* bezeichnet die Funktionalität weiteren Inhalt automatisch nachzuladen und ist beispielsweise auf YouTube vorzufinden. *Pull-to-Refresh* handelt von Interfaces, bei welchen Nutzer:innen eine Seite nach unten wischen müssen, um den Systemstatus zu aktualisieren. Es ist nicht vorhersehbar, ob bei der nächsten Aktualisierung neuer Inhalt geladen wird. Diese Ungewissheit kann Nutzer:innen dazu anregen, erneut nach unten zu wischen, um sicherzugehen nichts zu verpassen. Forscher:innen spekulieren, dass hierbei psychologische Phänomene ausgenutzt werden, auf welche Glücksspiele insbesondere Spielautomaten ebenfalls zurückgreifen (Monge Roffarello & Russis, 2022, 2 f.).

6 Vorkommen von Dark Patterns

Eine von der EU durchgeführte Studie ergab, dass Dark Patterns häufig von Anbieter:innen eingesetzt werden. Dabei untersuchten sie die 75 meistverwendeten Webseiten und Applikationen von EU-Bürger:innen aus den Bereichen E-Commerce, Unterhaltung, Gesundheit und Fitness, Tourismus, soziale Medien und Suchmaschinen. Aus den Ergebnissen geht hervor, dass 97% der Webseiten und Applikationen mindestens ein Dark Pattern verwenden (EK et al., 2022, 41 ff.). Dieses Kapitel beschränkt sich auf die Bereiche E-Commerce, Online-Tourismus und soziale Medien und analysiert Dark Patterns, die in diesen Bereichen angewendet werden. Dabei ist anzumerken, dass die nachfolgend beschriebenen Dark Patterns möglicherweise mittlerweile in den Unternehmen, in denen sie identifiziert wurden, nicht mehr vorkommen.

6.1 E-Commerce und Onlinemarktplätze

Mehrere Studien belegen, dass Dark Patterns in Online-Shops gängig eingesetzt werden. Beispielsweise identifizierten Mathur et al. (2019) auf 11 000 Shopping-Webseiten 1 818 Dark Pattern Instanzen. Ebenso spürte eine Studie der EK et al. (2022) Dark Patterns bei ausgewählten Online-Shops auf. Im Konkreten analysierte die Studie, in welchem Umfang bestimmte Arten von Dark Patterns vorkommen. Abbildung 11 gibt an, wie viele der 29 Online-Shops Gebrauch von den unten angeführten Dark Patterns machen. Aus der Studie geht hervor, dass die meisteingesetzten Dark Patterns der untersuchten Online-Shops *Hidden Information/False Hierarchy*, *Countdown Timer/Limited Time Message*, *Preselection* und *Roach Motel* umfassen (EK et al., 2022, S. 46).

Studien wie jene von Mathur et al. (2019, S. 14) oder der EK et al. (2022, S. 47) zeigen auf, dass in Onlineshops häufig Dark Patterns, die eine Dringlichkeit vermitteln, eingesetzt werden. Zu diesen Dark Patterns zählen Zeitdruck-Elemente wie *Countdown Timer* und *Low Stock/ High Demand Message*. Zeitdruck-Elemente können auf Produktseiten in Form von Deadlines auf kurzfristige Rabatte und Abverkäufe deuten. Auf Warenkorbseiten können sie ebenso auf zeitbegrenzte Reservierungen weisen, wie beispielsweise mit der Meldung „*Ihr Warenkorb wird in 10:00 Minuten ablaufen, bitte gehen Sie jetzt zur Kasse*“ (Mathur et al., 2019, S. 14).

Der Fast-Fashion Anbieter Shein nutzt beispielsweise Dark Patterns, die zeitlichen und sozialen Druck ausüben. Wie in Abbildung 12 ersichtlich, setzt das Unternehmen auf

diverse zeitbegrenzte Aktionen, Blitzangebote und Countdown Timer. Zudem bezweckt Shein mit der Meldung „Schnell! Fast ausverkauft…“ ebenfalls einen schnelleren Kaufabschluss (AK, 2023, S. 19).

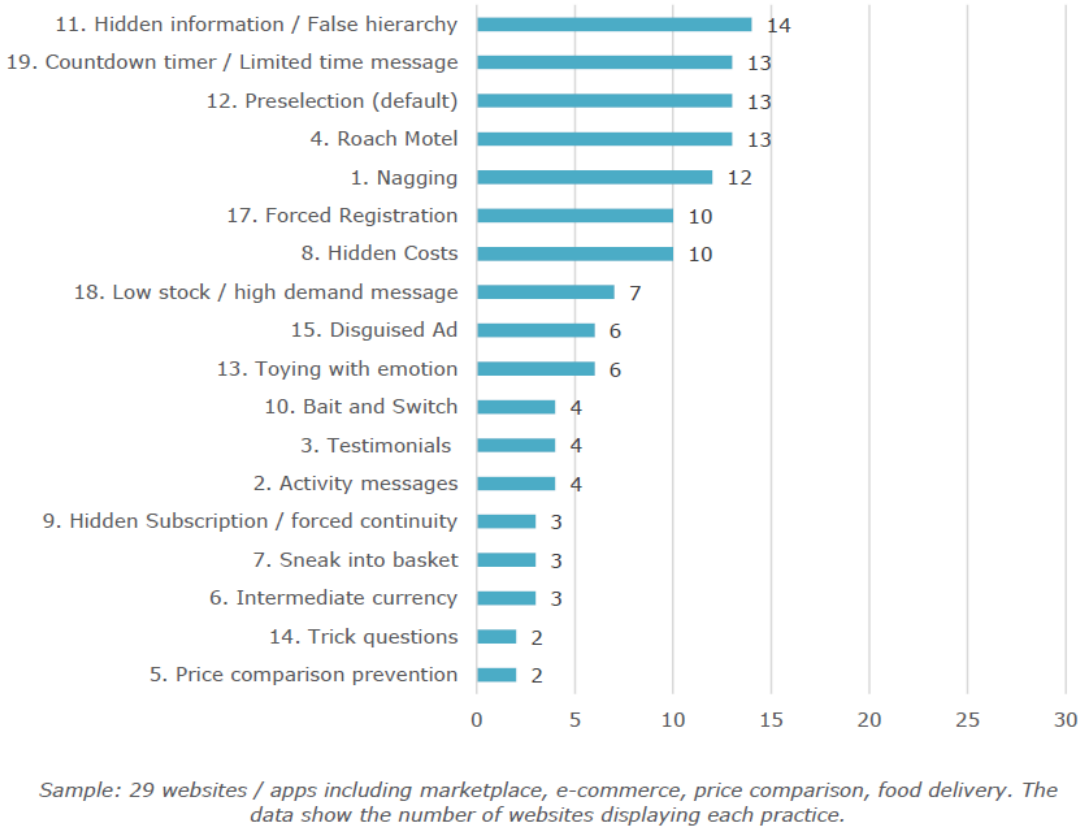

Abbildung 11: Gefundene Dark Patterns im Bereich des E-Commerce (Europäische Kommission [EK] et al., 2022, S. 45)

Solche Anzeigen sind häufig nicht wahrheitsgetreu. Mathur et al. (2019, S. 15) deckten in ihrer Studie 157 irreführende Countdown-Timer auf 140 Shopping-Webseiten auf. Ebenso führt die Studie der EK et al. (2022) an, dass auf Shein einige Blitzangebote vorgetäuscht sind, da dieselben Produkte nach der Deadline zum selben Preis weiterhin angeboten werden (EK et al., 2022, S. 47).

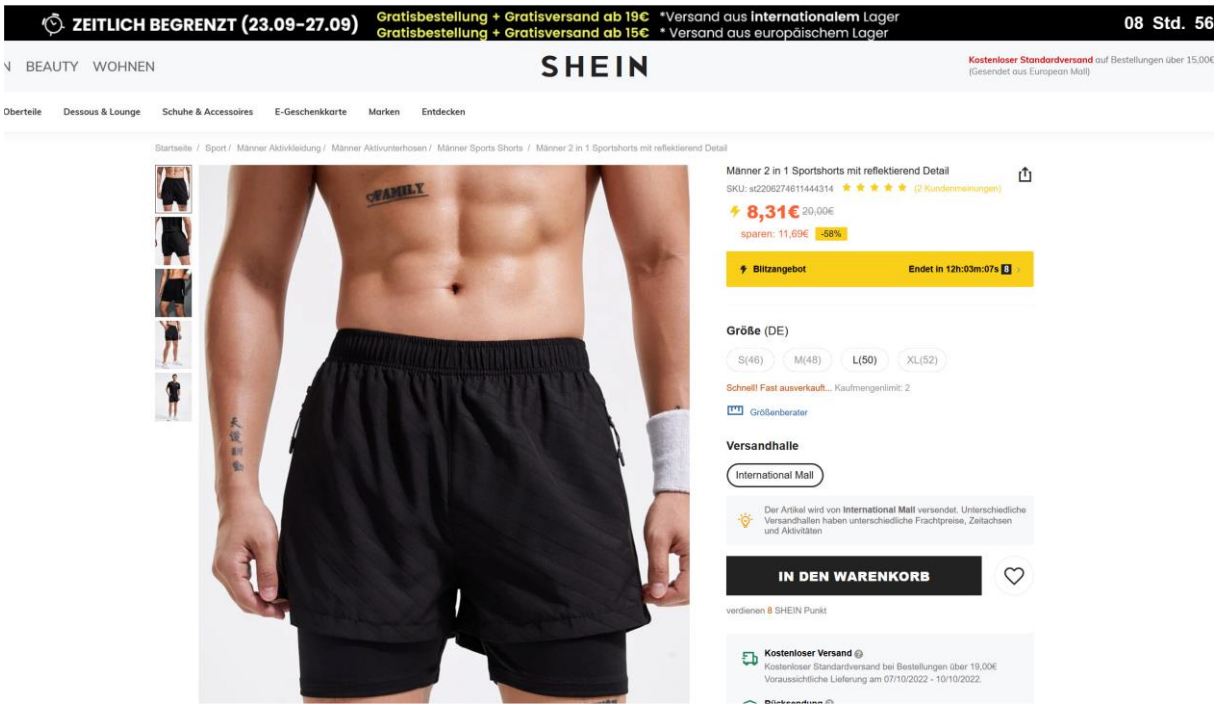

Abbildung 12: Shein nutzt viele Elemente, die zeitlichen Druck ausüben (AK, 2023, S. 20)

Weiters können mit dem Dark Pattern *Forced Registration* viele Onlineshops Nutzer:innen zwingen ein Konto zu erstellen, um alle Funktionen und Dienste freizuschalten. Der Studie der EK et al. (2022) zufolge konnte dieses Dark Pattern auf Onlinemarktplätze wie Allegro, Zalando und Deliveroo aufgefunden werden (EK et al., 2022, S. 47). Ebenfalls stellte eine Studie der AK fest, dass der Sportbekleidungshändler Fabletics auf das Dark Pattern zurückgreift (AK, 2023, S. 16). Eine Registrierung bei den oben angeführten Onlinehändlern ist für Nutzer:innen unumgänglich, um Käufe zu tätigen und im Falle von Fabletics eine Voraussetzung, um überhaupt die Produkte einsehen zu können (AK, 2023, S. 17; EK et al., 2022, S. 47).

Studien haben weiters Instanzen von *Hidden Subscription/ Forced Continuity* auf Onlineshops wie Zalando, Corte Ingles, Amazon und Fabletics identifiziert. So gibt Amazon auf ihrer Warenkorbseite an, dass Kund:innen, die mit der Amazon Visa Karte zahlen, eine Gutschrift von 40 Euro erhalten und enthält Kund:innen vor, dass ein Jahr nach der Kartenaktivierung eine Gebühr von 20 Euro jährlich zu zahlen ist (EK et al., 2022, S. 47). In Fabletics besteht die Möglichkeit Produkte als VIP in den Warenkorb zu legen, was um ein Vielfaches billiger ist als der Standardeinkauf. Wird jedoch für

die VIP-Option entschieden, so wird unbemerkt ein Vertrag mit einer monatlichen Gebühr von 54,95 Euro abgewickelt (AK, 2023, S. 17).

Viele Onlineshops nutzen darüber hinaus das Dark Pattern *Roach Motel*, um Konsument:innen die Deaktivierung ihres Accounts zu erschweren. Darunter fallen Unternehmen wie Worten, Continente, Zalando, LeroyMerlin und Amazon. Bei einigen dieser Händler ist es sogar nicht möglich das Konto eigenständig zu schließen. Stattdessen müssen Konsument:innen für eine erfolgreiche Kündigung den Kundenservice kontaktieren (EK et al., 2022, S. 47). Laut der Studie der AK (2023) gestaltet Shein ebenfalls das Löschen des Kontos kompliziert. Unter dem Reiter „Konto“ ist die Löschfunktion auf dem ersten Blick nicht ersichtlich, da diese durch den Link „Mehr ansehen“ versteckt wird. Wird die Löschfunktion getätigt, so ist es erforderlich drei Tage zu warten, bis die Deaktivierung abgeschlossen ist (AK, 2023, S. 21).

Das Dark Pattern *Hidden Costs* wird ebenfalls in Onlineshops geläufig eingesetzt. Google Shopping, Aliexpress, Corte Ingles, Uber Eats und Deliveroo bezwecken damit, anfallende Zusatzkosten bis zum Zahlungsprozess zu verbergen (EK et al., 2022, 47 f.). Auch der Blumeneinzelhändler ProFlowers (Abbildung 13) verrechnet im letzten Schritt hohe Lieferkosten, Steuern und Servicepauschalen (Mathur et al., 2019, S. 13).

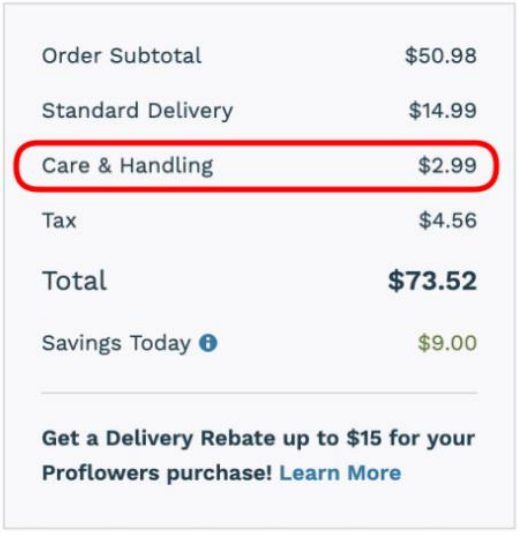

Abbildung 13: In ProFlowers werden die versteckten Kosten erst an der Kassa offenbart (Mathur et al., 2019)

6.2 Reise und Transport

Die Digitalisierung von Reiseanbietern hat in den letzten Jahrzehnten einen deutlichen Zuwachs erfahren. Im Jahre 2017 betrug der Umsatz der Online-Reisebürobranchen weltweit mehr als 629 Billionen US-Dollar. Im Jahre 2018 fielen Reiseunterkünfte unter die zweit meistgekauften Waren und Dienstleistungen in der Online-Umgebung (EK et al., 2020, S. 20). Eine Studie der EK et al. (2020, S. 24) zeigt auf, dass innerhalb der EU die meist besuchten Webseiten von Reiseanbietern, Booking.com, RentalCars, Airbnb, Ryanair und Trivago umfassen. Weiters geht aus der Studie hervor, dass die am häufigsten benutzten Applikationen von Reiseanbietern, Booking.com, Ryanair, Airbnb, TripAdvisor und Wizz Air miteinschließen (EK et al., 2020, S. 26).

Aufgrund der hohen Konkurrenz innerhalb des Reisemarkts ist es verlockend, Dark Patterns zu nutzen, um die Kaufbereitschaft der Konsument:innen zu erhöhen. Eine Studie der EK et al. (2022) zeigt auf, dass viele der bekannten Reiseanbieter:innen Dark Patterns einsetzen. Abbildung 14 veranschaulicht die Anzahl an Webseiten und Applikationen von Reiseanbieter:innen, die Gebrauch von den angeführten Dark Patterns machen. Es ist ersichtlich, dass nahezu alle der fünf untersuchten Webseiten und Applikationen auf mindestens ein Dark Pattern zurückgreifen.

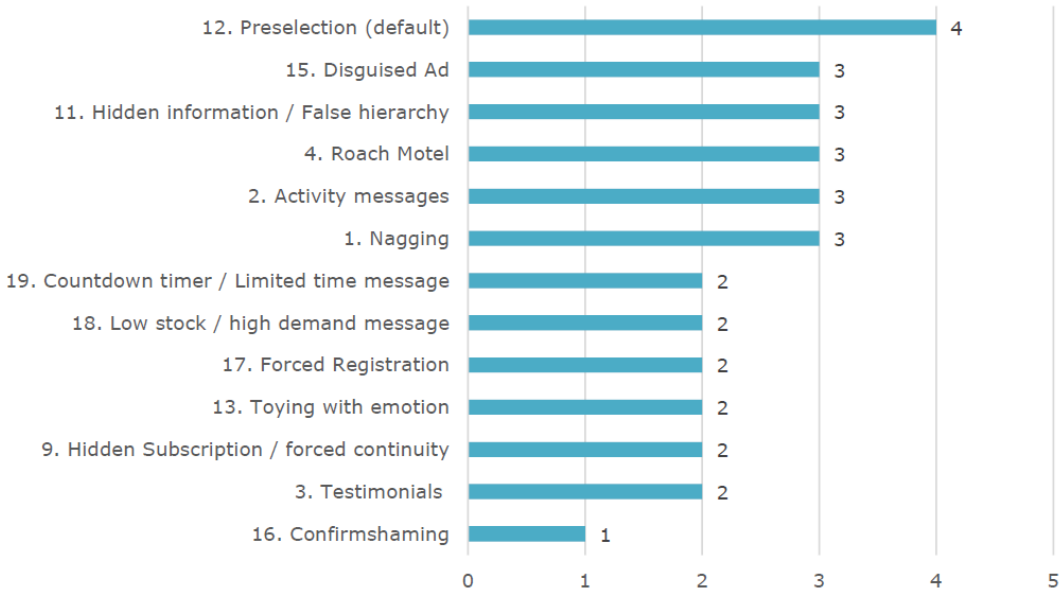

Abbildung 14: Gefundene Dark Patterns im Bereich des Online-Tourismus (Europäische Kommission [EK] et al., 2022, S. 54)

Reiseanbieter:innen können mithilfe von Dark Patterns, die auf Knappheit und Zeitbegrenzung deuten, die Kaufentscheidungen der Konsument:innen beeinflussen. Diese sind unter anderem auf Booking.com, Airbnb und Expedia präsent (EK et al., 2020, S. 54). Abbildung 15 und Abbildung 16 veranschaulichen einige solcher Instanzen auf Booking.com.

Durch Meldungen wie „Nur 1 Zimmer auf unserer Seite übrig“ oder „5-mal gebucht in den letzten 24 Stunden“ können Kund:innen fälschlicherweise den Eindruck gewinnen, dass die Unterkünfte in Kürze ausgebucht sein werden. Damit werden Kund:innen gedrängt, ihre Buchungen unverzüglich zu tätigen. Dennoch wird oft zu einem späteren Zeitpunkt festgestellt, dass die gleichen Unterkünfte immer noch zur Verfügung stehen (EK et al., 2020, S. 39).

Abbildung 16: *Limited Time Message* auf Booking.com (Booking.com)

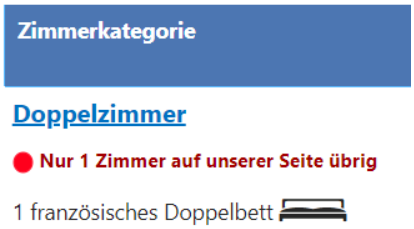

Abbildung 15: *Low Stock Message* auf Booking.com (Booking.com)

Ein Ausschnitt von Booking.com aus dem Jahr 2017 veranschaulicht, wie das Unternehmen anfallende Zusatzkosten (*Hidden Costs*) vor Interessent:innen versteckte. In Abbildung 17 wird der vermeintliche Gesamtpreis in großer und fettgedruckter Schrift hervorgehoben. Hier ist anzumerken, dass zusätzliche Gebühren nicht miteinberechnet wurden. Dagegen werden der tatsächliche Betrag und die Zusatzkosten in einer deutlich kleineren Schrift unterhalb aufgelistet. Mit dieser Taktik können Kund:innen in die Irre geführt werden, einen niedrigeren Preis zu zahlen (UXP2 Dark Patterns, 2023).

Eine Studie der EK et al. (2020, S. 41) führt an, dass Anwendungen von Fluggesellschaften, wie Rynair oftmals keine Option für einen kostenfreien Sitzplatz anbieten, was meistens einen Preisaufschlag von mindestens vier Euro zur Folge hat (*Hidden Costs*). Es ist jedoch erwähnenswert, dass Rynair inzwischen eine transparentere Darstellung von Sitzplatzoptionen eingeführt hat, wie in Abbildung 18 ersichtlich.

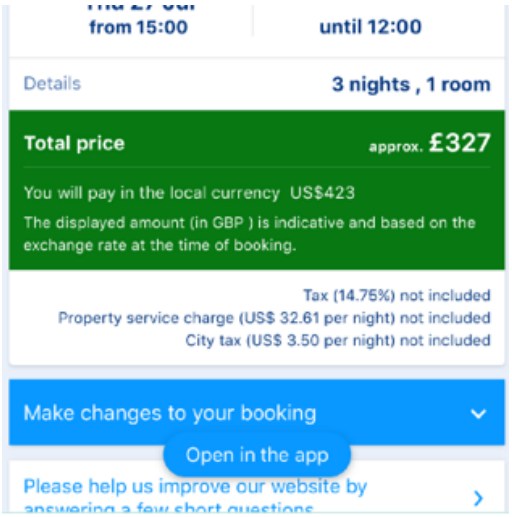

Abbildung 17: *Hidden Costs* auf Booking.com (UXP2 Dark Patterns, 2023)

Abbildung 18: Eine transparentere Darstellung der Sitzplatzoptionen (Ryanair.com, 2023)

Ein weiteres Dark Pattern, welches 2018 in der Ryanair App entdeckt wurde, ist in Abbildung 20 dargestellt. Hier würden Nutzer:innen, die ihre Suchkriterien abschicken, gleichzeitig den Nutzungsbedingungen der Webseite zustimmen. Die Information kann leicht übersehen werden, da sie in kleingedruckter Schrift unterhalb der gelben Schaltfäche zu finden ist.

Rynair nutzt ebenfalls Dark Patterns der Kategorie *Interface Interference*. Als Beispiel dient hierbei Abbildung 19. Bei der Auswahl von Reisegepäckstücken, werden die teureren Optionen mit kräftigeren Farben hervorgehoben, während die günstigste Option mit einem Grauton eher in den Hintergrund rückt.

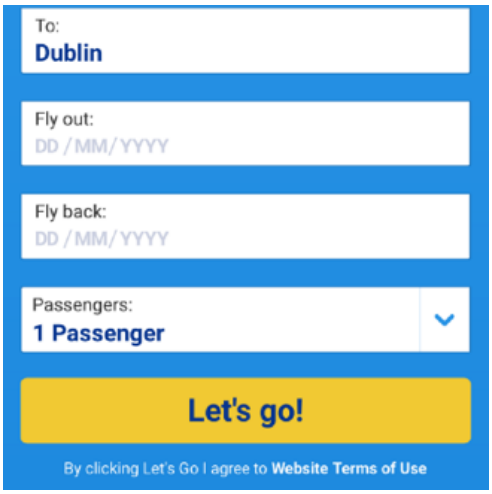

Abbildung 20: Forced Action/ Sneaking auf Ryanair (UXP2 Dark Patterns, 2023)

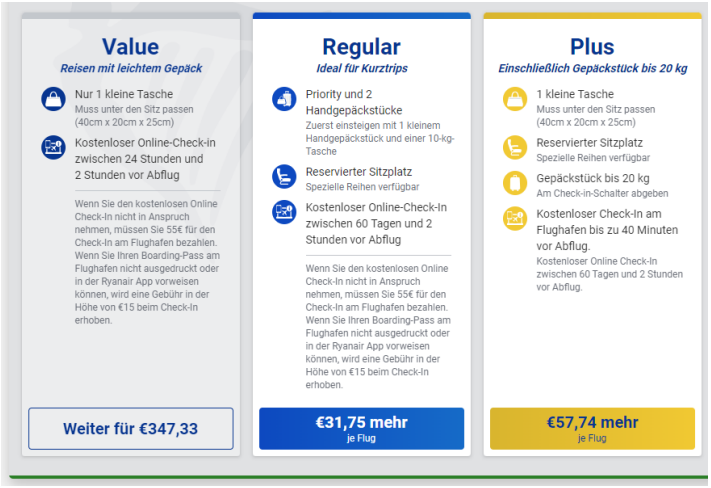

Abbildung 19: *False Hierarchy* auf Ryanair (Ryanair.com, 2023)

6.3 Soziale Medien

In der heutigen Zeit sind soziale Medien für viele Menschen unverzichtbar. Im Jahr 2022 verbrachten Menschen weltweit betrachtet im Durchschnitt mehr als zwei Stunden täglich auf sozialen Medienplattformen (Statista, 2022). Die Anzahl der Nutzer:innen sozialer Medienplattformen liegt im Millionenbereich. Im selben Jahr zählten Facebook (457 Millionen), Instagram (281 Millionen), TikTok (228 Millionen), LinkedIn (174 Millionen) und Pinterest (130 Millionen) zu den führenden sozialen Medienplattformen in Bezug auf die Nutzerzahl (Statista, 2023).

Eine Studie der EK identifizierte auf diversen sozialen Medienplattformen Dark Patterns (EK et al., 2022, S. 50). In Abbildung 21 sind Dark Patterns, die auf ausgewählten sozialen Medien wie unter anderem Facebook, TikTok, Pinterest und Instagram gefunden wurden, dargestellt.

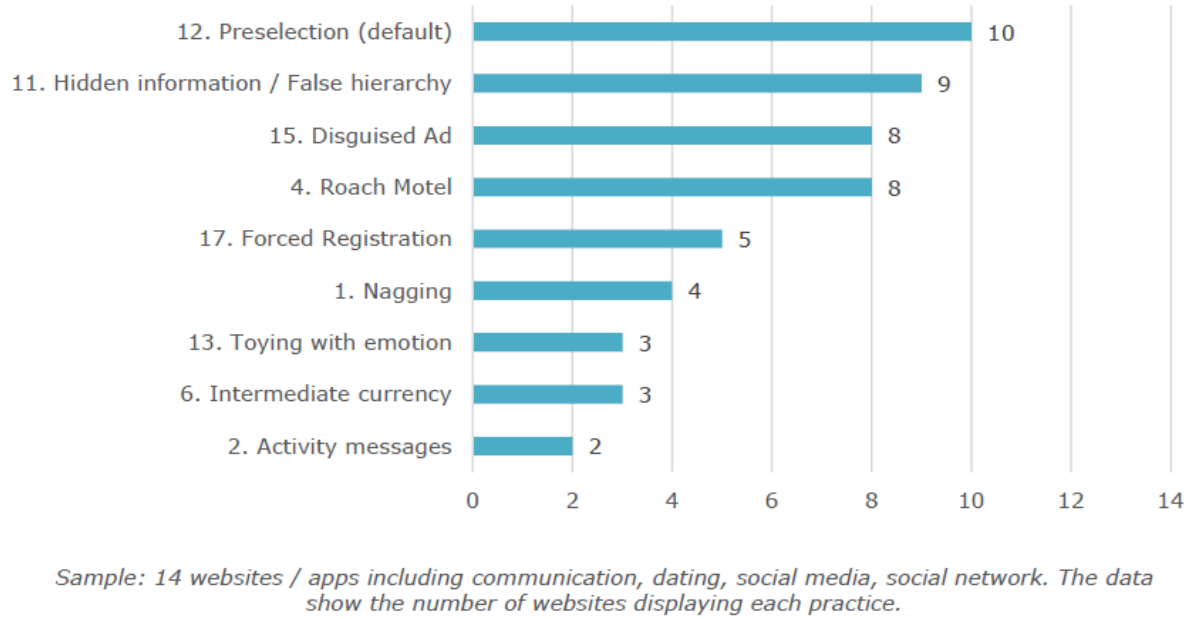

Abbildung 21: Gefundene Dark Patterns im Bereich der sozialen Medien (EK et al., 2022, S. 50)

Aus Abbildung 21 geht hervor, dass unter den untersuchten sozialen Medienplattformen *Preselection* das am häufigsten verwendete Dark Pattern ist. Facebook kombiniert beispielsweise dieses Dark Pattern mit *Obstruction* (Abbildung 22). Dabei macht es Facebook einfach, der Datenverarbeitung zuzustimmen, aber umständlich, sie abzulehnen. Die Zustimmung kann in einem Schritt erfolgen, während für die Ablehnung

zunächst die Einstellungen geöffnet, dann der Umschalter deaktiviert und schließlich die Änderung gespeichert werden muss (Brignull, 2010).

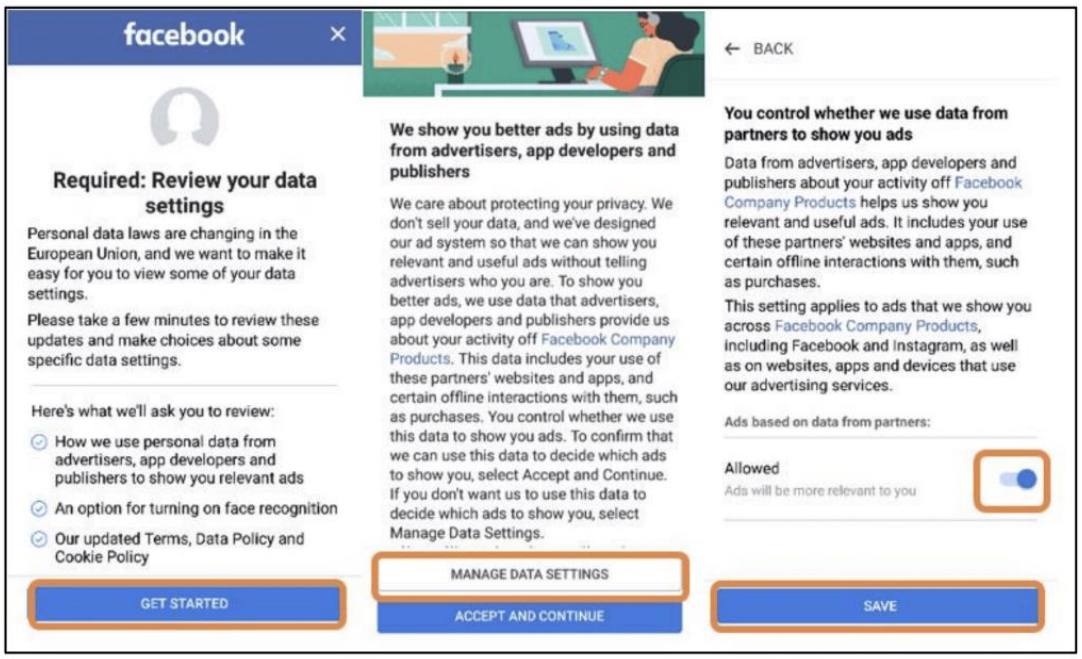

Abbildung 22: Facebook kombiniert *Obstruction* und *Preselection* (Brignull, 2010)

Die Studie entdeckte ebenso mehrere Fälle von versteckter Werbung (*Disguised Ads*) auf sozialen Medien wie Facebook, Instagram und Pinterest. Konkret handelt es sich um gesponserte Inhalte, die den Anschein erwecken, von Nutzer:innen selbst geteilt worden zu sein, wie beispielsweise in Abbildung 23 dargestellt (EK et al., 2022, S. 50).

Darüber hinaus wurden Instanzen von *Forced Registration* festgestellt. Auf Instagram und Pinterest ist es beispielsweise nicht möglich, den Inhalt einzusehen, ohne vorher einen Account anzulegen. Auf Facebook haben Nutzer:innen ohne Registrierung nur eingeschränkten Zugriff auf die Funktionalitäten (EK et al., 2022, S. 50).

Weiters trat in einigen Fällen das Dark Pattern *Roach Motel* zum Vorschein. Für das Löschen eines Kontos auf Facebook war es für Nutzer:innen aufgrund der Komplexität nötig ein Tutorial anzuschauen. Auf Instagram kann in der mobilen Applikation keine entsprechende Schaltfläche zum Löschen des Kontos gefunden werden; es gibt lediglich eine Funktion, um ein Konto vorübergehend zu deaktivieren. Um ein Konto endgültig zu löschen, mussten Nutzer:innen zur entsprechenden Webseite navigieren (EK et al., 2022, S. 50).

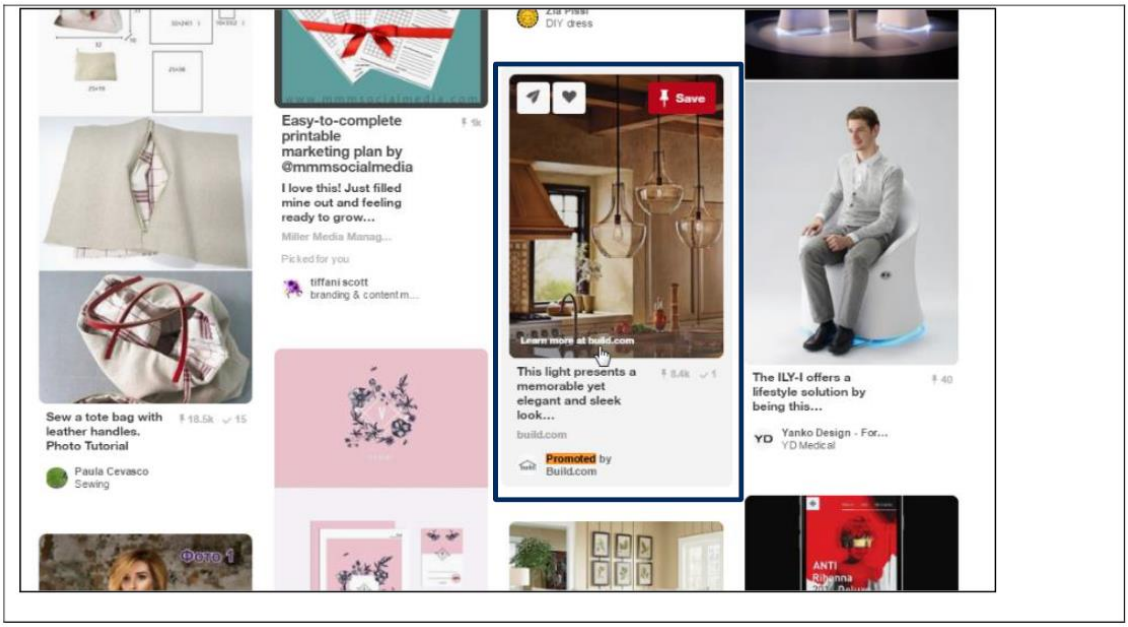

Abbildung 23: *Disguised Ad* auf Pinterest (EK, 2018, S. 32)

Auf Tiktok wurde zudem das Dark Pattern *Intermediate Currency* identifiziert. Konkret können Nutzer:innen ihr Geld gegen virtuelles Geld eintauschen, mit dem sie virtuelle Geschenke für andere Nutzer:innen kaufen können. Diese Taktik kann dazu führen, dass Nutzer:innen zum Kauf von Gegenständen verleitet werden, deren tatsächlicher Wert ihnen nicht bekannt ist (EK et al., 2022, S. 51).

LinkedIn wandte 2015 die Strategie *Forced Action* an. Während des Registrierungsprozesses forderte LinkedIn Nutzer:innen auf, ihre E-Mail-Adresse anzugeben, um Personen zu finden, mit denen sie sich vernetzen können. Wie in Abbildung 24 ersichtlich, wurde dabei die „Continue“-Schaltfläche stärker hervorgehoben als die Option „Skip this step“, wodurch Nutzer:innen den Eindruck vermittelt bekamen, dass die Angabe verpflichtend sei. Problematisch war auch, dass die angegebene E-Mail Adresse nicht nur genutzt wurde, um existierende LinkedIn Profile zu finden, sondern auch um Zugriff auf alle Kontakte der Nutzer:innen zu bekommen (Brignull, 2010). Mit der in Abbildung 25 dargestellten Benutzeroberfläche wurden Nutzer:innen zusätzlich dazu verleitet, Einladungsmails an jene Kontakte zu senden, die kein LinkedIn-Profil besaßen. Dabei hatte die Funktion „Add to network“ tatsächlich den Effekt, dass an alle markierten Kontakte eine E-Mail verschickt wurde (Dan Schlosser, 2015).

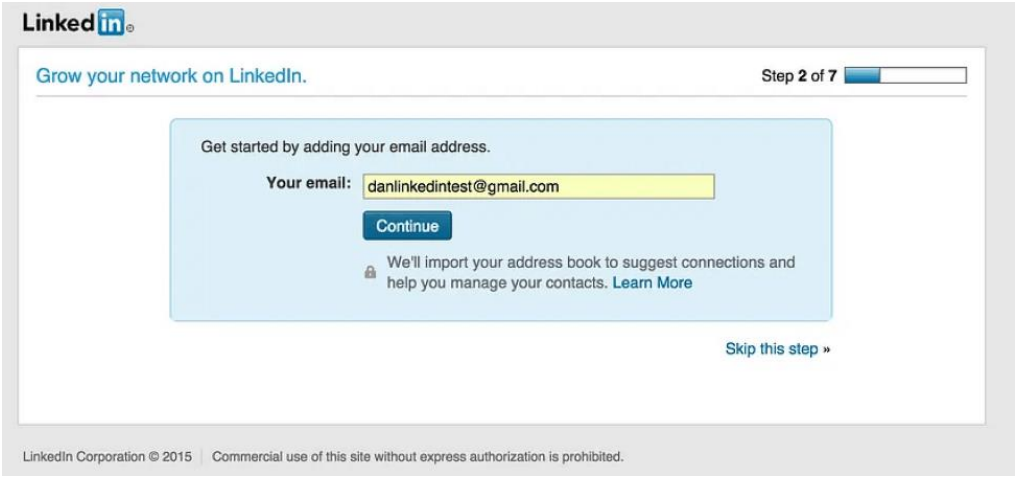

Abbildung 24: Benutzeroberfläche erweckt den Eindruck, dass die Angabe der E-Mail-Adresse zwingend erforderlich ist (Brignull, 2010)

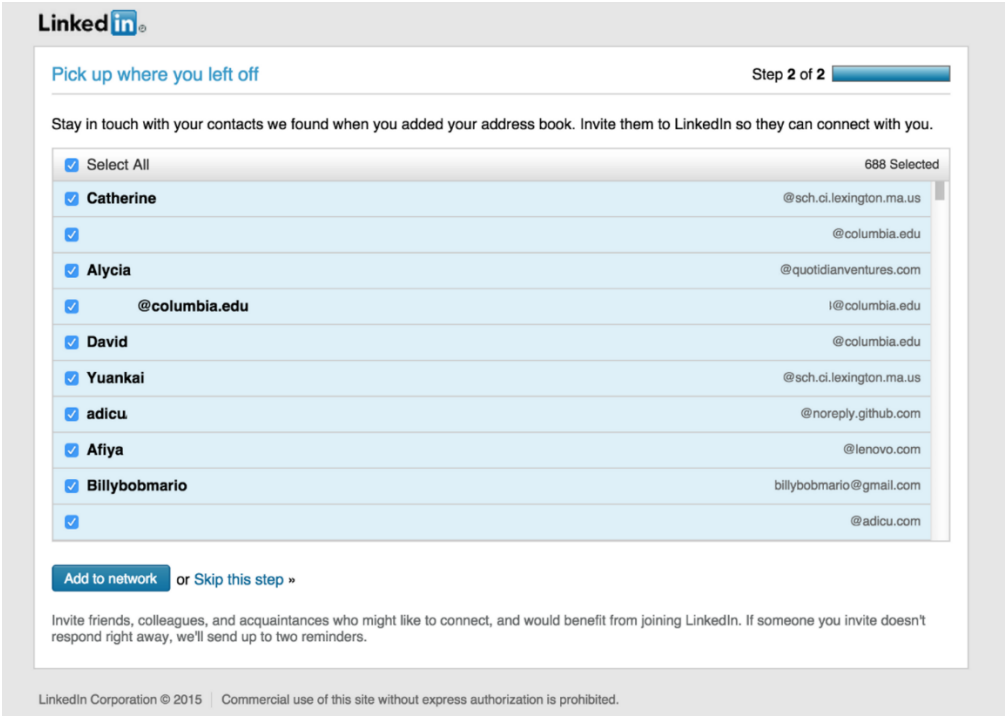

Abbildung 25: „Add to network“ fügt keine bestehenden LinkedIn Profile hinzu, sondern versendet Einladungsmails an jene markierten Personen (Dan Schlosser, 2015)

7 Rechtliche Situation

Im vorliegenden Kapitel wird untersucht, welche rechtlichen Maßnahmen auf der europäischen Ebene ergriffen werden, um Dark Patterns zu regulieren. Es werden relevante Gesetzgebungen vorgestellt, die darauf abzielen, den Einsatz von Dark Patterns einzuschränken und ihre Auswirkungen einzudämmen.

7.1 Charta der Grundrechte

Die Regulierung von Dark Patterns durch Gesetze, Verordnungen und Richtlinien baut auf einigen grundlegenden Rechten auf, die in der Grundrechtecharta (GRC) der EU (GRC, 2012) verankert sind. Diese betreffen den Schutz der Privatsphäre (GRC, 2012, Art 7) und persönlichen Daten (GRC, 2012, Art 8) sowie die Wahrung der Informationsfreiheit (GRC, 2012, Art 11), die Nichtdiskriminierung (GRC, 2012, Art 21) und den Verbraucherschutz (GRC, 2012, Art 38).

7.2 Das Paket des Digital Services Act

Das Paket des Digital Services Act wurde im Juli 2022 durch das Europäische Parlament angenommen. Es umfasst das Gesetz über den digitalen Markt (VO (EU) 2022/1925) und das Gesetz über digitale Dienste (VO (EU) 2022/2065), welche im November 2022 in Kraft traten. Beide Gesetze haben zum Ziel die Grundrechte der GRC in der Online-Umgebung zu wahren und faire Wettbewerbsbedingungen im Binnenmarkt zu schaffen (EK, 2023). Damit spielen diese eine große Rolle für die Regulierung der Dark Patterns.

7.2.1 Gesetz über den digitalen Markt (DMA)

Der DMA richtet sich an große Online-Plattformen, sogenannte *Torwächter*, die Plattformdienste bereitstellen, um Anbieter:innen und Endnutzer:innen zu vernetzen (VO (EU) 2022/1925, ErwGr 3). Ein Unternehmen gilt beispielsweise als Torwächter, wenn es „[…] *in jedem der vergangenen drei Geschäftsjahre in der Union einen Jahresumsatz von mindestens 7,5 Mrd. EUR erzielt hat* […]“ (VO (EU) 2022/1925, Art 3 Abs 2 a) oder „[…] *im vergangenen Geschäftsjahr mindestens 45 Millionen in der Union niedergelassene oder aufhältige monatlich aktive Endnutzer und mindestens 10 000 in der Union niedergelassene jährlich aktive gewerbliche Nutzer hatte* […]“ (VO (EU) 2022/1925, Art 3 Abs 2 b).

Der Begriff *Dark Patterns* wird im DMA nicht explizit genannt, jedoch implizieren einige Gesetzesstellen die Regulierung jener. Torwächtern ist es untersagt, die in der Verordnung festgelegten Verpflichtungen aus den Artikeln 5, 6 und 7 auf anderem Wege zu umgehen (VO (EU) 2022/1925, Art 13 Abs 4). Dazu zählen

> […] *die vom Torwächter verwendete Gestaltung, die Darstellung der Wahlmöglichkeiten des Endnutzers in einer nicht neutralen Weise oder die Nutzung der Struktur, der Funktion oder der Art und Weise der Bedienung einer Benutzerschnittstelle oder eines Teils davon, um die Nutzerautonomie, die Entscheidungsfindung oder die Wahlmöglichkeit zu beeinträchtigen oder einzuschränken.* (VO (EU) 2022/1925, ErwGr 70)

Das Konzept des Dark Patterns *Roach Motel* (4.3.2) wird im DMA reguliert. Um die Kündigung von Diensten zu erleichtern, fordert Artikel 13 folgendes:

> *Die allgemeinen Bedingungen des Torwächters für die Kündigung eines zentralen Plattformdienstes dürfen nicht unverhältnismäßig sein. Der Torwächter stellt sicher, dass die Kündigungsbedingungen ohne übermäßige Schwierigkeiten eingehalten werden können.* (VO (EU) 2022/1925, Art 13)

Daraus ergibt sich, dass das Kündigen eines Plattformdienstes genauso unkompliziert verlaufen muss, wie das Abonnieren desselben. So soll es Nutzer:innen möglich sein ihr erstelltes Konto ohne Umwege zu deaktivieren (VO (EU) 2022/1925, ErwGr 63). Neben dem einfachen Kündigen soll es ebenfalls möglich sein, Einwilligungen zur Verarbeitung personenbezogener Daten mühelos zu verweigern bzw. zu widerrufen. Der DMA legt dabei insbesondere Augenmerk auf die Gestaltung der Benutzeroberfläche:

> *Torwächter sollten ihre Online-Schnittstellen nicht so gestalten, organisieren oder betreiben, dass Endnutzer getäuscht, manipuliert oder anderweitig in ihrer Fähigkeit, ihre Einwilligung frei zu erteilen, maßgeblich beeinträchtigt oder behindert werden. Insbesondere sollte es Torwächtern nicht gestattet sein, Endnutzer mehr als einmal jährlich aufzufordern, ihre Einwilligung für denselben Verarbeitungszweck zu erteilen, für den sie ursprünglich keine Einwilligung erteilt oder ihre Einwilligung widerrufen haben.* (VO (EU) 2022/1925, ErwGr 37)

Der letzte Satz schließt Instanzen der Dark Pattern Kategorie *Nagging* mit ein. Laut Artikel 5 Absatz 10 (VO (EU) 2022/1925) wären demnach wiederholt auftauchende Pop-up-Fenster, die Nutzer:innen gegen ihren Willen, um die Angabe bestimmter Daten oder die Aktivierung bestimmter Berechtigungen bitten, untersagt.

7.2.2 Gesetz über digitale Dienste (DSA)

Im Gegensatz zum DMA, welcher sich ausschließlich an große Online-Plattformen richtet, enthält der DSA Vorschriften für eine umfangreichere Bandbreite an digitalen Dienste. Im Konkreten gilt diese Verordnung für „[…] *Vermittlungsdienste, die für Nutzer mit Niederlassungsort oder Sitz in der Union angeboten werden, ungeachtet des Niederlassungsortes des Anbieters dieser Vermittlungsdienste*“ (VO (EU) 2022/2065, Art 2 Abs 1). Damit schließt der DSA alle Dienste, die ein Online-Geschäft betreiben und die von Nutzer:innen bereitgestellten Informationen in einem Kommunikationsnetz übermitteln und speichern, wie E-Commerce-Plattformen und Social-Media-Netzwerke, mit ein (VO (EU) 2022/2065, Art 3g).

Der DSA führt im Erwägungsgrund 67 den Begriff *Dark Patterns* an und fordert ein Verbot dieser Praktiken:

> *Anbietern von Online-Plattformen sollte es […] untersagt sein, die Nutzer in die Irre zu führen oder zu etwas zu verleiten und die Autonomie, die Entscheidungsfreiheit oder die Auswahlmöglichkeiten der Nutzer durch den Aufbau, die Gestaltung oder die Funktionen einer Online-Schnittstelle oder eines Teils davon zu verzerren oder zu beeinträchtigen.* (VO (EU) 2022/2065, ErwGr 67)

Artikel 25 führt ausdrücklich ein Verbot von diesen Online-Schnittstellen an:

> *Anbieter von Online-Plattformen dürfen ihre Online-Schnittstellen nicht so konzipieren, organisieren oder betreiben, dass Nutzer getäuscht, manipuliert oder anderweitig in ihrer Fähigkeit, freie und informierte Entscheidungen zu treffen, maßgeblich beeinträchtigt oder behindert werden.* (VO (EU) 2022/2065, Art 25 Abs 1)

In diesem Zusammenhang werden *ausbeuterische Gestaltungsmuster* genannt, mit denen Anbieter:innen von Online-Plattformen auf Kosten der Interessen der Nutzer:innen, Vorteile für sich selbst erzielen. Dazu zählt die nicht neutrale Präsentation von Auswahlmöglichkeiten durch die bewusste Hervorhebung von visuellen, akustischen

oder sonstigen Elementen bestimmter Auswahlmöglichkeiten. Weiters sollen Praktiken, die unter *Nagging* und *Obstruction* fallen, untersagt werden. So dürfen Anbieter:innen Nutzer:innen nicht wiederholt dazu auffordern, eine bereits getroffene Auswahl zu treffen. Auch soll der Widerruf eines Dienstes nicht unverhältnismäßig schwieriger oder zeitaufwendiger gestaltet sein als die entsprechende Anmeldung. Der Abbruch von Käufen soll möglich und unkompliziert sein und Nutzer:innen dürfen nicht zu ungewollten Kaufentscheidungen irregeführt werden. Nutzer:innen dürfen auch nicht durch schwer änderbare Standardeinstellungen beeinflusst werden. Alles in allem dürfen Anbieter:innen die Autonomie sowie die Entscheidungsfreiheit der Nutzer:innen nicht untergraben (VO (EU) 2022/2065, ErwGr 67). Der DSA macht jedoch auch darauf aufmerksam, dass Anbieter:innen nicht daran gehindert werden sollen neue oder zusätzliche Dienste zu werben:

> *Rechtmäßige Praktiken – beispielsweise in der Werbung –, die mit dem Unionsrecht im Einklang stehen, sollten an sich nicht als Dark Patterns angesehen werden. Diese Vorschriften über Dark Patterns sollten dahin ausgelegt werden, dass sie verbotene Praktiken erfassen, die in den Anwendungsbereich dieser Verordnung fallen* […]. (VO (EU) 2022/2065, ErwGr 67)

7.3 Richtlinie über unlautere Geschäftspraktiken (UGP-RL)

Die UGP-RL zielt darauf ab Rechtsvorschriften hinsichtlich unlauterer Geschäftspraktiken innerhalb der Mitgliedstaaten zu vereinheitlichen und ein hohes Maß an Verbraucherschutz zu gewähren (RL 2005/29/EG, Art 1). Im Konkreten verbietet die Richtlinie den Einsatz von unlauteren Geschäftspraktiken „[…] *vor, während und nach Abschluss eines auf ein Produkt bezogenen Handelsgeschäfts*“ (RL 2005/29/EG, Art 3 Abs 1). Einige unlautere Geschäftspraktiken finden sich in Dark Patterns wieder. Daher kann die UGP-RL ebenfalls für die Regulierung von Dark Patterns bedeutsam sein.

7.3.1 Definition: unlautere Geschäftspraktik

Artikel 2d (RL 2005/29/EG) enthält eine umfassende Definition des Begriffs *Geschäftspraktiken*, die wie folgt formuliert ist:

> *[…] jede Handlung, Unterlassung, Verhaltensweise oder Erklärung, kommerzielle Mitteilung einschließlich Werbung und Marketing eines Gewerbetreibenden, die*

unmittelbar mit der Absatzförderung, dem Verkauf oder der Lieferung eines Produkts an Verbraucher zusammenhängt. (RL 2005/29/EG, Art 2d)

Nach jener breit gehaltenen Definition und der Interpretation, dass Praktiken nicht zwingend einen Kauf herbeiführen müssen, würden viele Dark Patterns, die für kommerzielle Zwecke eingesetzt werden, unter *Geschäftspraktiken* fallen (EK et al., 2022, S. 70).

Als eine unlautere Geschäftspraktik gilt laut Artikel 5 Absatz 2 (RL 2005/29/EG) jene Praktik, die „[…] *den Erfordernissen der beruflichen Sorgfaltspflicht widerspricht*“ und „[…] *in Bezug auf das jeweilige Produkt das wirtschaftliche Verhalten des Durchschnittsverbrauchers* […] *wesentlich beeinflusst oder dazu geeignet ist, es wesentlich zu beeinflussen*“. Damit zählen Praktiken, die von Anbieter:innen bewusst eingesetzt werden, um Konsument:innen zu einer uninformierten Entscheidung in einer wirtschaftlichen Situation zu veranlassen, die sie andernfalls nicht getroffen hätten, als unlauter. Darunter fallen insbesondere irreführende und aggressive Praktiken (RL 2005/29/EG, Art 4).

7.3.1.1 Irreführende und aggressive Geschäftspraktiken

Eine Geschäftspraktik wird in erster Linie als irreführend bezeichnet, „[…] *wenn sie falsche Angaben enthält und somit unwahr ist* […]“ (RL 2005/29/EG, Art 6 Abs 1). Weiters kann eine Praktik als irreführend eingestuft werden, wenn die Präsentation inhaltlich richtiger Angaben, wie unter anderem hinsichtlich der Verfügbarkeit des Produktes oder des Preises Verbraucher täuscht (RL 2005/29/EG, Art 6 Abs 1). Zudem gilt eine Praktik, die „[…] *wesentliche Informationen vorenthält, die der durchschnittliche Verbraucher je nach den Umständen benötigt, um eine informierte geschäftliche Entscheidung zu treffen* […]“ (RL 2005/29/EG, Art 7 Abs 1) oder „[…] *wesentliche Informationen* […] *verheimlicht oder auf unklare, unverständliche, zweideutige Weise oder nicht rechtzeitig bereitstellt oder wenn er den kommerziellen Zweck der Geschäftspraxis nicht kenntlich macht*“ (RL 2005/29/EG, Art 7 Abs 2) ebenfalls als irreführend.

Aggressive Geschäftspraktiken sind hingegen jene, die die Autonomie der Konsument:innen „[…] *durch Belästigung, Nötigung,* […] *oder durch unzulässige Beeinflussung* […]“ (RL 2005/29/EG, Art 8) einschränken. Darunter fällt unter anderem der Einsatz von drohenden oder beleidigenden Ausdrucksweisen (RL 2005/29/EG, Art 9b)

und die Schaffung von Hindernissen zur Kündigung eines Vertrags (RL 2005/29/EG, Art 9d).

7.3.2 Liste der unlauteren Geschäftspraktiken

Anhang 1 der UGP-RL führt eine Liste von irreführenden und aggressiven Geschäftspraktiken, die unter allen Umständen als unlauter gelten, an. Diese richtet sich hauptsächlich an Offline-Praktiken. Dennoch können einige davon in Dark Patterns übergeführt werden (EK et al., 2022, S. 71).

Die Punkte 5, 6 und 20 behandeln Lockangebote und die Bait-and-Switch-Technik. Auf diese Praktiken wird ebenfalls in der Online-Umgebung zurückgegriffen und ist unter dem Dark Pattern *Bait-and-Switch* bekannt. Punkt 7 beschreibt die Praxis, bei der Konsument:innen fälschlicherweise mitgeteilt wird, dass das Produkt zeitlich begrenzt oder unter bestimmten Bedingungen verfügbar sei. Diese Vorgehensweise gleicht den in der Online-Umgebung eingesetzten Dark Patterns der Kategorie *Urgency*, wie *Countdown-Timer* oder *Low Stock/ High Demand Message*. Weiters können Punkt 11 auf *Disguised Ad*, Punkt 26 auf *Nagging* und Punkt 29 auf *Sneak into Basket* abgestimmt werden (EK et al., 2022, S. 71).

Andere Dark Patterns, die nicht explizit aufgelistet sind, können ebenfalls gemäß Artikel 6 bis 9 (RL 2005/29/EG) als irreführende oder aggressive Praktiken eingestuft werden. So könnten beispielsweise laut Artikel 6 Absatz 1 Buchstabe d (RL 2005/29/EG) *Hidden Costs*, *Price Comparison Prevention* und *Intermediate Currency* und laut Artikel 7 Absatz 1f (RL 2005/29/EG) *Hidden Information*, *False Hierarchy* und *Trick Questions* als irreführend bezeichnet werden. Ferner könnten *Obstruction* bzw. *Roach Motel* und *Forced Continuity* unter aggressive Praktiken fallen (RL 2005/29/EG, Art 9d).

7.4 Datenschutz-Grundverordnung (DSGVO)

Das vorrangige Ziel der DSGVO besteht darin, den Schutz personenbezogener Daten zu gewährleisten und gleichzeitig den freien Datenverkehr zu ermöglichen (VO (EU) 2016/679, Art 1 Abs 1). Sie legt Grundsätze für die Verarbeitung personenbezogener Daten fest, wie unter anderem „*Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz*“ (VO (EU) 2016/679, Art 5 Abs 1 lit a), „*Zweckbindung*“ (VO (EU)

2016/679, Art 5 Abs 1 lit b) und „*Datenminimierung*“ (VO (EU) 2016/679, Art 5 Abs 1 lit c). Zudem gewährt die DSGVO den betroffenen Personen Rechte, wie das Recht auf Widerruf einer Einwilligung (VO (EU) 2016/679, Art 21) und das Recht auf Einsicht in alle Informationen „[…] *in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache* […]“ (VO (EU) 2016/679, Art 12 Abs 1). Die DSGVO verpflichtet weiters Verantwortliche, den Datenschutz durch Technikgestaltung (*data protection by design*) und durch datenschutzfreundliche Voreinstellungen (*data protection by default*) zu gewährleisten (VO (EU) 2016/679, ErwGr 78).

Verantwortliche, die in der EU niedergelassen sind, außerhalb der EU Dienstleistungen oder Waren für Einzelpersonen in der EU anbieten oder deren Verhalten in der EU überwachen, unterliegen der Regelungen der DSGVO (VO (EU) 2016/679, Art 3). Damit richtet sich die DSGVO an all jene, die die Verarbeitung personenbezogener Daten in Verbindung mit der EU durchführen.

7.4.1 Dark Patterns unter der DSGVO

Dark Patterns, die Einzelpersonen dazu verleiten, persönliche Daten preiszugeben, können gegen die Bestimmungen des Datenschutzgesetzes verstoßen (EK et al., 2022, S. 75). Insbesondere sind solche, die dazu führen, dass die Einwilligung entgegen ihrer Definition in Artikel 4 Absatz 11 (VO (EU) 2016/679) unfreiwillig erteilt wird, als rechtswidrig anzusehen, da die betroffenen Personen nicht ausreichend über die Umstände informiert wurden.

Die EK und der EDSA haben Benutzeroberflächen im Hinblick auf die in der DSGVO genannten Grundsätzen analysiert. Dabei ist *Fairness* ein übergreifendes Prinzip, welches sicherstellen soll, dass personenbezogene Daten nicht auf eine Weise verarbeitet werden, die die betroffenen Personen benachteiligt, diskriminiert, irreführt oder unerwartete negative Auswirkungen auf sie hat. Demnach würde eine Benutzeroberfläche, die dem Benutzer unzureichende oder irreführende Informationen über die Verarbeitung personenbezogener Daten liefert, gegen das Prinzip der Fairness verstoßen. Für die Analyse wurden neben Fairness weitere Grundsätze wie *Verantwortung*, *Transparenz* sowie die Verpflichtung, datenschutzfreundliche Gestaltung und Voreinstellungen sicherzustellen, berücksichtigt (EK et al., 2022, S. 75; EDSA, 2023, S. 11).

7.4.1.1 Fairness und Transparenz

Anbieter:innen sollen Fairness und Transparenz bei der Verarbeitung von personenbezogenen Daten einhalten. Laut Artikel 5 Absatz 1 Buchstabe a (VO (EU) 2016/679) müssen jene „*auf rechtmäßige Weise, nach Treu und Glauben und in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden*“. So müssen die für betroffene Personen relevanten Informationen hinsichtlich der Verarbeitung von Daten „*in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache*“ (VO (EU) 2016/679, Art 12 Abs 1) mitgeteilt werden.

Mehrere Dark Patterns missachten die in Artikel 5 Absatz 1 Buchstabe a und Artikel 12 Absatz 12 (VO (EU) 2016/679) erläuterten Bestimmungen, da Personen, die jenen ausgesetzt sind, im Unklaren sind, wie ihre Daten verarbeitet werden oder wie sie Kontrolle über die Verarbeitung erlangen können. Beispiele hierfür sind die Dark Patterns *Privacy Maze* oder *Too many options* (Nutzer:innen mit Optionen überladen). Jene weichen von den Grundsätzen der Fairness und Transparenz ab, da Nutzer:innen von der Gestaltung der Benutzeroberfläche überwältigt werden, wodurch sie mit hoher Wahrscheinlichkeit ihre Ziele aufgeben oder wichtige Informationen und Funktionen übersehen (EDSA, 2023, 65 f.). Nutzer:innen von wichtigen Datenschutzinformationen geschickt abzulenken, ist ein weiteres Dark Pattern, welches das Prinzip der Fairness und Transparenz nicht einhält. Dieses Dark Pattern ist unter dem Namen *Look over there* bekannt und hat zur Folge, dass Nutzer:innen durch Ablenkung auf ihre ursprüngliche Absicht vergessen (EDSA, 2023, 66 f.). Weiters dienen Dark Patterns wie *Emotional Steering* (Beeinflussung der Emotionen, sodass Nutzer:innen entgegen ihren Interessen hinsichtlich des Datenschutzes handeln), *Hidden in plain sight* (Verwendung von Designelementen, um Nutzer:innen zu datenschutzfeindlichen Optionen zu verleiten) (EDSA, 2023, S. 67), *Language discontinuity* (Datenschutzinformationen werden ausschließlich in einer Fremdsprache angezeigt), *Conflicting Information* (Anzeige von widersprüchlichen Datenschutzinformationen) und *Ambiguous wording or information* (Einsatz von vagen und zweideutigen Begriffen) ebenfalls als Beispiele für die Missachtung der Grundsätze Fairness und Transparenz (EDSA, 2023, 70 f.).

Die oben genannten Dark Patterns führen dazu, dass entweder die bereitgestellten Informationen oder das Design nicht den Verpflichtungen zur fairen und transparenten

Verarbeitung gemäß Artikel 12 Absatz 1 und Artikel 5 Absatz 1 Buchstabe a (VO (EU) 2016/679), entsprechen.

7.4.1.2 Zweckbindung

Entsprechend Artikel 5 Absatz 1 Buchstabe b (VO (EU) 2016/679) müssen personenbezogene Daten „*für festgelegte, eindeutige und legitime Zwecke erhoben werden und dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden*“. Diese Vorschrift wird mit dem Begriff „Zweckbindung“ kurzgefasst.

Dark Patterns, die Nutzer:innen überzeugen, mehr Daten als für den Zweck der Verarbeitung notwendig preiszugeben, stehen nicht im Einklang mit dem Prinzip der Zweckbindung. Das Dark Pattern *Continuous prompting* fällt darunter. Nutzer:innen werden dabei durch wiederholte Aufforderungen zur Dateneingabe oder Zustimmung zu einer neuen Zweckbestimmung gedrängt, mehr persönliche Daten anzugeben oder mehr Rechte zur Verarbeitung ihrer Daten zu erlauben als erforderlich (vgl. *Nagging*). Nutzer:innen geben oftmals nach und willigen ein, weil sie die Anfragen als störend empfinden und sie während der Nutzung der Dienste unterbrochen werden (EDSA, 2023, S. 65). Das Prinzip der Zweckbindung wird verletzt, wenn Nutzer:innen beispielsweise mehrfach aufgefordert werden, ihre Telefonnummer bekannt zu geben und fälschlicherweise behauptet wird, dass die Telefonnummer für Sicherheitsmaßnahmen, wie die Zwei-Faktor-Authentisierung, benötigt wird, obwohl sie tatsächlich für Werbezwecke vorgesehen ist (EDSA, 2023, S. 18).

7.4.1.3 Datenminimierung

Die DSGVO beschreibt den Grundsatz der Datenminimierung wie folgt: „*Personenbezogene Daten müssen dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein*“ (VO (EU) 2016/679, Art 5 Abs lit c). Das zuvor erwähnte Beispiel, in dem Nutzer:innen wiederholt aufgefordert werden, ihre Telefonnummer preiszugeben, verstößt nicht nur gegen das Prinzip der Zweckbindung, sondern auch gegen das Prinzip der Datenminimierung. Mit dem Dark Pattern *Deceptive Snugness* können ebenfalls mehr Daten als für den Verarbeitungszweck benötigt, gesammelt werden. Dabei werden Optionen, die die meisten Rechte erlauben, vorausgewählt. Weiteres können *Trick Questions* oder visuelle

Hervorhebungen als Beispiele dienen. All diese angeführten Gestaltungen, mit der Absicht Daten über das erforderliche Maß zu erheben, würden vom Grundsatz der Datenminimierung abweichen (EK et al., 2022, S. 77).

7.5 Verbraucherrechte-Richtlinie (VR-RL)

Die VR-RL lässt sich ebenfalls auf bestimmte Dark Patterns anwenden, um ihre Rechtmäßigkeit zu prüfen. Sie stellt sicher, dass Konsument:innen relevante Informationen vor Vertragsabschluss erhalten und das Recht haben, den Vertrag zu widerrufen (RL 2011/83/EU, ErwGr 9). Artikel 22 (RL 2011/83/EU) kann für die Dark Patterns *Preselection* und *Hidden Costs* bedeutsam sein und lautet wie folgt:

> *Bevor der Verbraucher durch den Vertrag oder das Angebot gebunden ist, hat der Unternehmer die ausdrückliche Zustimmung des Verbrauchers zu jeder Extrazahlung einzuholen* [...] *Hat der Unternehmer vom Verbraucher keine ausdrückliche Zustimmung eingeholt, sondern sie dadurch herbeigeführt, dass er Voreinstellungen verwendet hat, die vom Verbraucher abgelehnt werden müssen, wenn er die zusätzliche Zahlung vermeiden will, so hat der Verbraucher Anspruch auf Erstattung dieser Zahlung.* (RL 2011/83/EU, Art 22)

Es wird betont, dass Konsument:innen aktiv werden müssen, wenn sie finanzielle Entscheidungen treffen, und dass vorausgewählte Optionen keine explizite Zustimmung darstellen.

Ferner kann das Dark Pattern *Sneak into Basket* unter die Regelung von Artikel 27 (RL 2011/83/EU) fallen. Hier wird klargestellt, dass Konsument:innen nicht verpflichtet werden dürfen, für unbestellte Produkte aufzukommen. Insbesondere darf die fehlende Reaktion des Konsumenten nicht als Zustimmung zum Kauf des Produkts gewertet werden (RL 2011/83/EU, Art 27).

8 Empfehlungen für Gegenmaßnahmen

In diesem Kapitel werden potentielle Abwehrstrategien gegen Dark Patterns behandelt, die über die bloße Einhaltung gesetzlicher Vorschriften hinausgehen. Im ersten Teil werden Maßnahmen zur Unterstützung von Nutzer:innen vorgestellt. Im zweiten Teil stehen Handlungsempfehlungen für Unternehmen und Designer:innen im Vordergrund.

8.1 Ansätze zur Unterstützung von Konsument:innen

Nachfolgend werden verschiedene Ansätze, um die Kontrolle und Entscheidungsfähigkeit der Konsument:innen im Umgang mit Dark Patterns zu stärken, dargestellt. Es werden Strategien wie *Boosting*, der Einsatz von *Bright Patterns* und *Reflective Patterns* sowie Werkzeuge diskutiert, die dabei helfen sollen, Dark Patterns zu erkennen, zu vermeiden und ihnen entgegenzuwirken.

8.1.1 Boosting

Forscher:innen empfehlen die Entscheidungsfähigkeit der Konsument:innen zu fördern, welches auch unter dem Begriff *Boosting* bekannt ist. Damit sollen Nutzer:innen eine größere Kontrolle über ihre digitale Umgebung erhalten und sich wirksamer vor Dark Patterns schützen können. Beispielsweise können Konsument:innen eine Kontrollliste systematisch durchgehen, bevor sie eine Entscheidung treffen (OECD, 2022, S. 46). In diesem Zusammenhang rät die AK Konsument:innen, sich nicht stressen, erpressen und verunsichern zu lassen. Konsument:innen sollen ihre Kaufabsicht hinterfragen und sich vorübergehend von Stresssituationen distanzieren (AK Presseunterlage, S. 7).

8.1.2 Bright Patterns und Reflective Patterns

Eine andere Idee besteht darin, sogenannte *Bright Patterns* einzusetzen, die Konsument:innen unterschwellig zu Entscheidungen, die in ihrem eigenen Interesse liegen, bewegen. Allerdings werden einige Kritikpunkte an diesem Vorgehen angeführt. Zum einen ergibt es für Unternehmen wenig Sinn auf diese Praktiken zurückzugreifen, um beispielsweise die Privatsphäre der Nutzer:innen zu schützen, da ihre Ziele in der Regel von denen der Nutzer:innen abweichen. Es ist daher anzuzweifeln, dass Unternehmen tatsächlich *Bright Patterns* anwenden Zum anderen setzt diese Vorgehensweise

ebenfalls voraus, dass keine freie Entscheidungsfindung von Nutzer:innen zugelassen wird. Forscher:innen sehen dies als problematisch, da es Nutzer:innen erschwert wird, zu lernen, aktiv zu werden und nach ihren Präferenzen zu agieren. Dagegen wird der Vorschlag gemacht, sogenannte *Reflective Patterns* einzusetzen, die wie der Name suggeriert, Nutzer:innen animieren, über ihre Entscheidungen zu reflektieren (EK et al., 2022, S. 115).

8.1.3 Werkzeuge

Mehrere Forscher:innen engagieren sich dafür, Werkzeuge wie Webseiten und Browser Erweiterungen zu entwickeln, um Bewusstsein für Dark Patterns zu schaffen, diese aufzuklären und Konsument:innen zu helfen, sich vor ihnen zu schützen.

8.1.3.1 Webseiten

Harry Brignull veröffentlichte im Rahmen seiner Deceptive Patterns Initiative eine Webseite[1], die Terminologien und Beispiele von Dark Pattern bereitstellt. Außerdem gibt es auf der Webseite die Möglichkeit eigens gefundene Dark Pattern Instanzen einzureichen, um so die Beispielsammlung zu vergrößern. Auf der Webseite befindet sich auch ein Abschnitt namens *Hall of Shame*. Dieser zeigt eine Sammlung von Dark Patterns an, die bei Unternehmen identifiziert wurden. Gleichzeitig werden damit Unternehmen, die häufig auf solche Praktiken zurückgreifen, an den Pranger gestellt. Auf eine ähnlichen Weise informieren Webseiten wie UXP² Dark Patterns[2], Dark Patterns Tip Line[3] und Dark Pattern Detection Project (DAPDE)[4] Konsument:innen und andere Stakeholder über Dark Patterns und ermöglichen es, gefundene Dark Patterns zu melden.

8.1.3.2 Browser Erweiterungen

Forscher:innen empfehlen Plug-ins zu verwenden, um sich Dark Patterns zur Wehr zu setzen. Dafür wurden einige Browser Erweiterungen entwickelt, wie CookieBlock und Consent-O-Matic. Mit CookieBlock[5] können Nutzer:innen ihre Cookie-Einstellungen festlegen und das Plug-in bestrebt alle Cookies zu löschen, die nicht mit ihrer Angabe

[1] https://www.deceptive.design/
[2] https://darkpatterns.uxp2.com/
[3] https://darkpatternstipline.org/
[4] https://dapde.de/de/
[5] https://github.com/dibollinger/CookieBlock

übereinstimmen. Consent-O-Matic[6] bemüht sich zusätzlich Cookie-Banners zu entfernen. Sobald die Cookie-Präferenzen bestimmt sind, füllt die Erweiterung die meisten dieser wiederkehrenden Formulare automatisch aus. Diese Plug-ins vermindern die Gefahr, dass die falsche Option unbeabsichtigt aufgrund irreführender Designs gewählt wird.

Mathur et al. (2019, S. 25) empfehlen Browser Erweiterungen zu entwickeln, die Dark Patterns aufspüren und kennzeichnen. Hierfür stellen sie die im Zuge ihrer Untersuchung entstandene Sammlung an Dark Patterns bereit. DAPDE geht auf diesen Vorschlag ein und hat den Dapde Pattern Highlighter[7] veröffentlicht. Dieser deckt mithilfe von KI-basierter Textanalyse automatisiert Dark Patterns auf, markiert diese und informiert Nutzer:innen, um welches Dark Pattern es sich dabei handelt.

8.2 Handlungsempfehlungen für Unternehmen und Designer:innen

Zusätzlich zu den Maßnahmen, die Konsument:innen dabei unterstützen, sich aktiv gegen Dark Patterns zu wehren, können Unternehmen und Designer:innen selbst einen Beitrag zur Bekämpfung von Dark Patterns leisten. Zu diesem Zweck werden nachfolgend verschiedene Ansätze und Empfehlungen für Unternehmen und Designer:innen vorgestellt, darunter der Einsatz von Metriken zur Messung von Langzeitfolgen, die Durchführung von Selbstaudits und die Anwendung von Richtlinien und Frameworks zur Förderung von ethischem Design.

8.2.1 Metriken für Langzeitfolgen in A/B-Tests und Selbstaudits

Viele Unternehmen führen A/B-Tests durch, um die Benutzeroberfläche ihrer Produkte zu verbessern. Dabei können im Laufe der Verbesserungen unbeabsichtigt Dark Patterns entstehen. Der Grund besteht darin, dass für A/B-Tests üblicherweise Metriken herangezogen werden, die für Unternehmen allein interessant sind. Eine Metrik wie die Click-through-rate (CTR) gibt keinen Aufschluss über langfristige Auswirkungen. Demnach kann eine Designänderung, die eine höhere CTR verursacht, gleichzeitig Kundenunzufriedenheit hervorrufen und letztendlich dazu führen, dass Nutzer:innen das Produkt ablehnen (Narayanan et al., 2020, S. 80). Forscher:innen raten daher ab,

[6] https://github.com/cavi-au/Consent-O-Matic
[7] https://github.com/Dapde/Pattern-Highlighter

A/B-Tests ausschließlich für die Steigerung der Konversionsrate zu verwenden. Unternehmen sollen ebenfalls die Interessen der Konsument:innen und die Einhaltung der Rechtsvorschriften berücksichtigen (OECD, 2022, S. 48). Narayanan et al. (2020) schlagen hierfür vor, für A/B-Tests mindestens eine Metrik, die Langzeitfolgen misst, zu wählen. So kann neben der CTR, zusätzlich die Nutzerbindung in Betracht gezogen werden (Narayanan et al., 2020, S. 80).

Darüber hinaus regen Forscher:innen Unternehmen an, die Entscheidungsarchitektur ihrer Benutzeroberflächen regelmäßig zu begutachten. Beispielsweise können Unternehmen sogenannt e Sludge Audits durchführen. Im Zuge dessen werden Designelemente, die für die Entscheidungsfindung der Konsument:innen relevant sind, auf Irreführung und Manipulation überprüft. Unternehmen können zudem Dashboards nutzen, um solche Sludges zu verwalten, zu verfolgen und zu verbessern (OECD, 2022, S. 48).

8.2.2 Ethik im Design und Selbstregulierung

Dark Patterns können nicht allein durch eine Liste von verbotenen Dark Patterns vermieden werden. Vielmehr sollen laut Narayanan et al. (2020, S. 81) Werte erarbeitet werden, nach denen man sich während dem Designprozess richtet. Dabei sollen diese Werte mit jenen, die für die Gesellschaft bedeutsam sind, bestmöglich in Einklang gebracht werden. Hierfür sollen Unternehmen ihre Wertvorstellungen kritisch überprüfen und gleichzeitig Feedback von Konsument:innen einholen. Autonomie und Privatsphäre sind beispielsweise Werte, die derzeit in Unternehmen nicht im gleichen Ausmaß wie in der Gesellschaft erstrebt werden und es bedarf einer Harmonisierung dieser Werte (Narayanan et al., 2020, S. 82).

Werte können als Grundlage für die Formulierung von Richtlinien dienen. Solche Richtlinien können Unternehmen helfen Eigeninitiativen zu ergreifen und gehen über gesetzliche Vorschriften hinaus. Angesichts der kontinuierlichen Weiterentwicklung von Dark Patterns rückt der Appell zur Selbstregulierung zunehmend in den Vordergrund. Denn die alleinige Regulierung durch Gesetze ist zu aufwendig und weniger flexibel (Narayanan et al., 2020, S. 84).

8.2.2.1 Richtlinien und Frameworks

Es wurden zahlreiche Frameworks und Richtlinien entwickelt, die Unternehmen bei der Schaffung von benutzerfreundlichen Systemen unterstützen. Beispielsweise stellt der *ICC Advertising and Marketing Communications Code* Standards für ethisches Verhalten bereit und regt Unternehmen an, verantwortungsbewusst zu handeln. Darüber hinaus soll die Notwendigkeit Gesetze zu verschärfen, minimiert werden (Internationale Handelskammer [ICC], 2018, S. 3). Im Kodex werden unter anderem folgende Forderungen in Bezug auf Konsument:innen aufgestellt:

1. Ehrliche und wahrheitsgemäße Kommunikation.
2. Kein Missbrauch des Vertrauens oder keine Ausnutzung der Unwissenheit.
3. Preisgeben aller für die Entscheidungsfindung relevanter Informationen.
4. Schutz der Privatsphäre.
5. Einsatz von echten Testimonials. (ICC, 2018, S. 9–14)

Mit dem *Corporate Digital Responsibility-Kodex* (CDR) verpflichten sich Unternehmen bei der Gestaltung von technischen Systemen freiwillig zu Verhaltensweisen, die das Wohl der Gesellschaft im Fokus haben (Bundesministerium für Umwelt, Naturschutz, nukleare Sicherheit und Verbraucherschutz [BMUV], 2021, S. 2). Der CDR-Kodex legt hierfür konkrete Zielsetzungen fest:

1. Gesellschaftliche Grundwerte.
2. Nutzen schaffen.
3. Schaden vermeiden.
4. Autonomie.
5. Fairness.
6. Transparenz.
7. Verantwortlichkeit.
8. Nachhaltigkeit. (BMUV, 2021, S. 3)

Die User Experience Professionals Association (UXPA) entwickelte ein Verhaltenskodex, welches Usability-Fachleute auffordert ethische Standards einzuhalten (User Experience Professionals' Association [UXPA], 2005, S. 1). Mitglieder:innen dieser Vereinigung müssen folgende Richtlinien dieses Verhaltenskodexes befolgen:

1. Handeln Sie im Interesse aller.

2. Seien sie mit jedermann ehrlich.
3. Richten Sie keinen Schaden an und, wenn möglich: Schaffen Sie Vorteile.
4. Handeln Sie rechtschaffen.
5. Vermeiden Sie Interessenkonflikte.
6. Respektieren Sie Datenschutz, Vertraulichkeit und Anonymität.
7. Stellen Sie alle erhobenen und ausgewerteten Daten bereit. (UXPA, 2005, S. 1)

Sollten Mitglieder:innen gegen diese Prinzipien verstoßen, behält sich die UXPA das Recht vor, sie von der Vereinigung auszuschließen (UXPA, 2005, S. 1).

Darüber hinaus klärt die Richtlinie der niederländischen Verbraucherschutzbehörde (ACM) über den Schutz von Konsument:innen in der digitalen Umgebung auf, wo die Grenze zwischen Überzeugung und Irreführung bei online Geschäftspraktiken liegt. Die Richtlinie legt ebenfalls nahe, wie Benutzerschnittstellen gestaltet werden können, sodass Kund:innen informierte und gerechte Entscheidungen treffen können (Netherlands Authority for Consumers and Markets [ACM], 2023). Die wichtigsten Prinzipien dieser Richtlinie lauten wie folgt:

1. Give complete information.
2. Give correct information.
3. Give easy-to-understand information.
4. Give the information before the consumer makes a purchase.
5. Make sure that the information is easy to find.
6. Make sure your environment is logical and fair.
7. Ensure the default settings are favorable to consumers.
8. Be mindful of the vulnerabilities of consumers.
9. Test the effects of your online choice architecture. (ACM, 2023)

Weiters veröffentlichte der EDSA eine Richtlinie über die Erkennung und Umgehung irreführender Designs in sozialen Medien. Sie führt an, welche Dark Patterns Vorschriften der DSGVO verletzen und veranschaulicht diese anhand von Anwendungsfällen. Die Richtlinie stellt ebenfalls *Best Practices* vor um Rechtsverstöße zu minimieren (EDSA, 2023, S. 3).

Die BMUV hat zusätzlich Leitlinien für die Gestaltung fairer und verbraucherfreundlicher Cookie-Banner erarbeitet. Eine der Anforderungen ist, dass neben „Alles

Akzeptieren“, auch die Option „Alles Ablehnen“ vorhanden sein muss und beide auf derselben Ebene platziert sein müssen (BMUV, 2023, S. 8).

9 Fazit und Ausblick

Dark Patterns sind bewusst gestaltete Benutzeroberflächen, die Nutzer:innen täuschen, manipulieren oder Handlungen aufzwingen. Sie heben sich von benutzerfreundlichem Design ab, da sie nicht zum Vorteil der Nutzer:innen entwickelt werden, sondern die Ziele der Unternehmen verfolgen, darunter um finanzielle Gewinne zu erzielen, Daten zu sammeln und die Aufmerksamkeit der Betroffenen zu beeinflussen.

Diese manipulativen und irreführenden Designs basieren auf den Erkenntnissen der Verhaltensökonomie und machen sich Heuristiken sowie Urteilsfehler zunutze. Insbesondere sind sie eng mit dem Konzept *Nudging* verknüpft, welches darauf abzielt, das Entscheidungsverhalten von Menschen zu beeinflussen. Darüber hinaus wurden einige Dark Patterns durch traditionelle Geschäftspraktiken inspiriert, wie beispielsweise die Praktik *Bait and Switch*. Hinzu kommt der Trend *Growth Hacking*, bei welchem mithilfe von Nudging und A/B-Tests kostengünstige und effektive Marketingtechniken entwickelt wurden. So entstanden allmählich die ersten Dark Patterns.

Eine Vielzahl von Wissenschaftler:innen hat sich darum bemüht, eine Typologie für Dark Patterns zu entwickeln. Allerdings besteht keine Einigung einer einheitlichen Typologie, da jene sich oftmals auf spezifische Kontexte wie den Datenschutz beziehen. Zudem ist es schwierig eine allumfassende Typologie zu erarbeiten, da voraussichtlich im Laufe der Zeit neue Dark Patterns entstehen werden. Die im Zuge dieser Arbeit erläuterten Dark Patterns zielen im Allgemeinen darauf ab, Nutzer:innen zu stören, Hindernisse zu stellen, relevante Informationen und Wahlmöglichkeiten vorzuenthalten, sie zu bestimmten Aktionen zu zwingen und mit ihren Emotionen zu spielen. Entsprechend fallen sie in eine oder mehrere der folgenden Kategorien: *Nagging*, *Obstruction*, *Sneaking*, *Interface Interference*, *Social Proof* und *Urgency*.

Durch Dark Patterns können Konsument:innen einen finanziellen Schaden davontragen. Dark Patterns, die fälschlicherweise auf die Warenknappheit und die Popularität eines Produkts deuten, führen beispielsweise dazu. Ebenso sind irreführende Kostendarstellungen, wie das verzögerte Anzeigen von hohen Zusatzkosten Beispiele. Darüber hinaus stellen Dark Patterns eine Bedrohung für die Privatsphäre der Konsument:innen dar. Mit wiederholter Aufforderung zur Eingabe von überflüssigen Daten,

schwer auffindbaren Kontrollmechanismen und von Unternehmen präferierten Voreinstellungen, sammeln sie ohne die ausdrückliche Zustimmung der Betroffenen Daten. Zusätzlich können Dark Patterns ein suchtähnliches Verhalten auslösen, indem sie kontinuierlich die Aufmerksamkeit der Konsument:innen aufrechterhalten. In diesem Zusammenhang verwenden Wissenschaftler:innen den Begriff *attention-capture Dark Patterns*, die nicht nur auf Benutzeroberflächenelemente beschränkt sind, sondern auch auf Funktionalitäten wie beispielsweise *Autoplay* miteinschließen.

Studien belegen, dass Dark Patterns in der Online-Umgebung weit verbreitet sind. Besonders viele Dark Patterns häufen sich im Bereich des E-Commerce bzw. der Onlinemarktplätze an. Darunter fallen viele, die einen zeitlichen bzw. sozialen Druck ausüben. Darüber hinaus werden auch andere Dark Patterns wie *Roach Motel*, *Nagging*, *Preselection* und *Hidden Information* gängig eingesetzt. Dark Patterns sind auch im Online-Tourismus häufig anzutreffen und erzeugen hier oft ein Gefühl der Dringlichkeit. Bekannte soziale Medienplattformen greifen ebenfalls auf Dark Patterns zurück. Im Gegensatz zu den beiden zuvor genannten Bereichen, setzen soziale Medienplattformen weniger auf Dark Patterns, die Dringlichkeit vermitteln sollen, sondern eher auf solche, die für einen komplexen Interaktionsablauf sorgen und relevante Informationen verstecken. Dadurch werden Konsument:innen dazu verleitet, ihre Daten preiszugeben.

Die Regulierung von Dark Patterns erstreckt sich über mehrere Gesetzgebungen. Aktuelle EU-Verordnungen wie der DMA und der DSA beinhalten Bestimmungen, die für Dark Patterns relevant sind. Während der DMA sich ausschließlich auf große Online-Plattformen konzentriert, berücksichtigt der DSA auch kleinere Online-Dienste. In beiden Verordnungen wird verdeutlicht, dass Anbieter:innen ihre Benutzeroberflächen nicht so gestalten dürfen, dass sie den Nutzer:innen ihre freie und informierte Entscheidungsmöglichkeit nehmen. So soll beispielsweise das Kündigen nicht schwieriger sein als die entsprechende Registrierung oder Unternehmen dürfen nicht Nutzer:innen ständig auffordern Einwilligungen zu erteilen, die sie ursprünglich abgelehnt haben. Auch ältere Rechtsnormen können zur Regulierung von Dark Patterns beitragen. Die UGP-RL legt ihren Fokus auf betrügerische Geschäftspraktiken und untersagt insbesondere irreführende und aggressive Vorgehensweisen. Darüber hinaus enthält sie eine Liste von Geschäftspraktiken, die auf jeden Fall verboten sind, wie zum Beispiel Lockvogelangebote, irreführende Dringlichkeitsmitteilungen und versteckte

Werbeanzeigen. Zusätzlich enthält die VR-RL relevante Vorschriften für die Regulierung einiger Dark Patterns. Im Konkreten kann sie Konsument:innen vor Dark Patterns schützen, die bei Vertragszustimmungen eingesetzt werden. Eine weitere wichtige Rolle spielt die DSGVO, da viele Dark Pattern Instanzen darauf abzielen, Daten zu sammeln. Dark Patterns, die gegen die Grundsätze der Fairness, Transparenz, Zweckbindung und Datenminimierung verstoßen, können gemäß der DSGVO verboten werden.

Die alleinige Regulierung durch Rechtsnormen erweist sich als unzureichend, um effektiv gegen Dark Patterns vorzugehen. Daher ist es ebenso wichtig, dass einerseits Schutzvorkehrungen für Konsument:innen getroffen werden und andererseits Unternehmen sowie Designer:innen verantwortungsbewusst handeln. Mithilfe von *Boosting* und *Reflective Patterns* können Konsument:innen zur Reflektion angeregt werden. Webseiten können Konsument:innen helfen sich über Dark Patterns zu informieren und mit Browser Erweiterungen können Dark Patterns gedämpft werden. Unternehmen sollen darüber hinaus A/B Tests durchführen, die Langzeitfolgen berücksichtigen und sich mittels Verhaltenskodexes selbst regulieren.

Die Auseinandersetzung mit Dark Patterns ist von großer Bedeutung, da sie viele Grundrechte der Betroffenen verletzen, insbesondere das Recht auf freie und informierte Entscheidungen. Es besteht Besorgnis darüber, dass Dark Patterns in naher Zukunft personalisiert werden (Narayanan et al., 2020, S. 79). Daten, die durch Dark Patterns gesammelt werden, könnten dies erleichtern. Zudem ist zu erwarten, dass im Laufe der Zeit neue Formen von Dark Patterns entstehen werden. Daher ist es wichtig, dass nicht nur Gesetzgebungen kontinuierlich aktualisiert werden, sondern Unternehmen Selbstinitiativen ergreifen, um diesen Entwicklungen gerecht zu werden. Damit tragen Unternehmen und Designer:innen eine erhebliche Verantwortung und sollten ihre Handlungen stets kritisch hinterfragen.

Literaturverzeichnis

Arbeiterkammer (2023). Verlorene Zeit, Verlorenes Geld: Dark Patterns im Alltag von Konsument:innen, 1–28. https://www.arbeiterkammer.at/beratung/konsument/HandyundInternet/Internet/Dark_Patterns.pdf

Avila, J. & Holding, R. (9. Februar 2009). Dannon Yogurt Faces Lawsuit Over False Advertising. *ABC News*. https://abcnews.go.com/TheLaw/story?id=4188726&page=1

Beck, H. (2014). *Behavioral Economics: Eine Einführung*. Christian Rieck Verlag.

Bindra, S., Sharma, D., Parameswar, N., Dhir, S. & Paul, J. (2022). Bandwagon effect revisited: A systematic review to develop future research agenda. *Journal of Business Research*, *143*, 305–317. https://doi.org/10.1016/j.jbusres.2022.01.085

Bizer, G. Y. & Schindler, R. M. (2005). Direct evidence of ending-digit drop-off in price information processing. *Psychology and Marketing*, *22*(10), 771–783. https://doi.org/10.1002/mar.20084

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*(4), 237–254. https://doi.org/10.1515/popets-2016-0038

Brasler, K. & Densmore, A. (2022). *Sale Prices Are Rarely Real Deals*. https://www.checkbook.org/national/sale-fail/

Brignull, H. (2010). *Deceptive Design*. https://www.deceptive.design

Bundesministerium für Umwelt, Naturschutz, nukleare Sicherheit und Verbraucherschutz (2021). Corporate Digital Responsibility-Kodex: Freiwillige Selbstverpflichtung mit Bericht, 1–10. https://cdr-initiative.de/kodex

Bundesministerium für Umwelt, Naturschutz, nukleare Sicherheit und Verbraucherschutz (2023). Good-Practice-Initiative für das Einwilligungsmanagement bei

Cookie-Bannern: Design-Leitlinien. https://www.bmuv.de/download/guidelines-fuer-eine-nutzerfreundliche-cookie-banner-gestaltung

Cadwalladr, C. & Graham-Harrison, E. (2018). *Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach*. https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election

Cohen, S. (2018). Manipulation and Deception. *Australasian Journal of Philosophy*, *96*(3), 483–497. https://doi.org/10.1080/00048402.2017.1386692

Conti, G. & Sobiesk, E. (2010). Malicious interface design. In M. Rappa, P. Jones, J. Freire & S. Chakrabarti (Hrsg.), *Proceedings of the 19th international conference on World wide web* (S. 271–280). ACM. https://doi.org/10.1145/1772690.1772719

Crain, M. (2018). The limits of transparency: Data brokers and commodification. *New Media & Society*, *20*(1), 88–104. https://doi.org/10.1177/1461444816657096

Dan Schlosser. (2015). *Linkedin Dark Patterns*. https://schlosser.io/writing/linkedin-dark-patterns/

Europäische Kommission. (2018). *Behavioural study on advertising and marketing practices in online social media: Final report*. Luxembourg. GfK Belgium; Europäische Kommission. https://doi.org/10.2818/290217

Europäische Kommission. (2023). *Das Paket des Digital Services Act*. https://digital-strategy.ec.europa.eu/de/policies/digital-services-act-package

Europäische Kommission, Exekutivagentur für Verbraucher, Gesundheit, Landwirtschaft und Lebensmittel, Lupiáñez-Villanueva, F., Montealegre Olaya, A. F. & Bogliacino, F. (2020). *Behavioural Study on Advertising and Marketing Practices in Travel Booking Websites and Apps: Final Report*. https://data.europa.eu/doi/10.2818/728775

Europäische Kommission, Generaldirektion Justiz und Verbraucher, Francisco, L.-V., Alba, B. & Francesco, B. (2022). *Behavioural study on unfair commercial*

practices in the digital environment : dark patterns and manipulative personalisation : final report: Final Report. https://data.europa.eu/doi/10.2838/859030

Charta der Grundrechte der Europäischen Union, Amtsblatt der Europäischen Union 391 (2012). https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=celex%3A12012P%2FTXT

Europäischer Datenschutzausschuss (EDSA) (14. Februar 2023). *Guidelines 03/2022 on deceptive design patterns in social media platform interfaces: how to recognise and avoid them* (Richtlinie 03/2022). Brüssel.

Richtlinie 2005/29/EG des Europäischen Parlaments und des Rates vom 11. Mai 2005 über unlautere Geschäftspraktiken im binnenmarktinternen Geschäftsverkehr zwischen Unternehmen und Verbrauchern und zur Änderung der Richtlinie 84/450/EWG des Rates, der Richtlinien 97/7/EG, 98/27/EG und 2002/65/EG des Europäischen Parlaments und des Rates sowie der Verordnung (EG) Nr. 2006/2004 des Europäischen Parlaments und des Rates (Richtlinie über unlautere Geschäftspraktiken), Amtsblatt der Europäischen Union 22. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32005L0029

Richtlinie 2011/83/EU des Europäischen Parlaments und des Rates vom 25. Oktober 2011 über die Rechte der Verbraucher, zur Abänderung der Richtlinie 93/13/EWG des Rates und der Richtlinie 1999/44/EG des Europäischen Parlaments und des Rates sowie zur Aufhebung der Richtlinie 85/577/EWG des Rates und der Richtlinie 97/7/EG des Europäischen Parlaments und des Rates, Amtsblatt der Europäischen Union 64. https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=celex%3A32011L0083

Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung), Amtsblatt der Europäischen Union 1. https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=uriserv%3AOJ.L_.2016.119.01.0001.01.DEU&toc=OJ%3AL%3A2016%3A119%3ATOC

Verordnung (EU) 2022/1925 des Europäischen Parlaments und des Rates vom 14. September 2022 über bestreitbare und faire Märkte im digitalen Sektor und zur Änderung der Richtlinien (EU) 2019/1937 und (EU) 2020/1828 (Gesetz über digitale Märkte), Amtsblatt der Europäischen Union 1. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022R1925

Verordnung (EU) 2022/2065 des Europäischen Parlaments und des Rates vom 9. Oktober 2022 über einen Binnenmarkt für digitale Dienste und zur Änderung der ichtlinie 2000/31/EG (Gesetz über digitale Dienste), Amtsblatt der Europäischen Union 1. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022R2065&qid=1666857835014

Eurostat (2. Februar 2022). Online shopping ever more popular. *Eurostat*. https://ec.europa.eu/eurostat/web/products-eurostat-news/-/ddn-20220202-1

Favaretto, M., Clercq, E. de & Elger, B. S. (2019). Big Data and discrimination: perils, promises and solutions. A systematic review. *Journal of Big Data*, *6*(1). https://doi.org/10.1186/s40537-019-0177-4

Gray, C. M., Kou, Y., Battles, B., Hoggatt, J. & Toombs, A. L. (2018). The Dark (Patterns) Side of UX Design. In R. Mandryk, M. Hancock, M. Perry & A. Cox (Hrsg.), *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems* (S. 1–14). ACM. https://doi.org/10.1145/3173574.3174108

Haita-Falah, C. (2017). Sunk-cost fallacy and cognitive ability in individual decision-making. *Journal of Economic Psychology*, *58*, 44–59. https://doi.org/10.1016/j.joep.2016.12.001

Hansen, P. G., Skov, L. R., Jespersen, A. M., Skov, K. L. & Schmidt, K. (2016). Apples versus brownies: A field experiment in rearranging conference snacking buffets to reduce short-term energy intake. *Journal of Foodservice Business Research*, *19*(1), 122–130. https://doi.org/10.1080/15378020.2016.1129227

Hanson, J. D. & Kysar, D. A. (1999). Taking Behavioralism Seriously: The Problem of Market Manipulation. *NYUL rev*, *74*, 630–749.

Harvard. (2023). *The Anchoring Effect and How it Can Impact Your Negotiation*. https://www.pon.harvard.edu/daily/negotiation-skills-daily/the-drawbacks-of-goals/

Herpen, E. van, Pieters, R. & Zeelenberg, M. (2005). How Product Scarcity Impacts on Choice: Snob and Bandwagon Effects. *Advances in Consumer Research*, *32*, 623–624.

Holiday, R. (2012). *Everything Is Marketing: How Growth Hackers Redefine The Game*. https://www.fastcompany.com/3003888/everything-marketing-how-growth-hackers-redefine-game

Internationale Handelskammer (2018). ICC Advertising and Marketing Communications Code: Building consumer trust through responsible marketing. https://iccwbo.org/news-publications/policies-reports/icc-advertising-and-marketing-communications-code

Johnson, E. J., Bellman, S. & Lohse, G. L. (2002). Defaults, Framing and Privacy: Why Opting In-Opting Out. *Marketing Letters*, *13*, 5–15.

Kahn, C. M. & Roberds, W. (2008). Credit and identity theft. *Journal of Monetary Economics*, *55*(2), 251–264. https://doi.org/10.1016/j.jmoneco.2007.08.001

Kahneman, D. (2012). *Schnelles Denken, langsames Denken* (T. Schmidt, Übers.) (1. Aufl.). Siedler.

Levin, I. P. & Gaeth, G. J. (1988). How Consumers are Affected by the Framing of Attribute Information Before and After Consuming the Product. *Journal of Consumer Research*, *15*(3), 374–378.

Levin, S. (1. Mai 2017). Facebook told advertisers it can identify teens feeling 'insecure' and 'worthless'. *The Guardian*. https://www.theguardian.com/technology/2017/may/01/facebook-advertising-data-insecure-teens

Lukoff, K., Lyngs, U., Zade, H., Liao, J. V., Choi, J., Fan, K., Munson, S. A. & Hiniker, A. (2021). How the Design of YouTube Influences User Sense of Agency. In Y. Kitamura, A. Quigley, K. Isbister, T. Igarashi, P. Bjørn & S. Drucker

(Hrsg.), *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems* (S. 1–17). ACM. https://doi.org/10.1145/3411764.3445467

Madrian, B. C. & Shea, D. F. (2001). The Power of Suggestion: Inertia in 401(k) Participation and Savings Behavior. *The Quarterly Journal of Economics*, *116*(4), 1149–1187.

Maitland, G. D. (1996). *Manipulation der peripheren Gelenke* (2. Aufl.). *Rehabilitation und Prävention: Bd. 20*. Springer.

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*, *3*(CSCW), 1–32. https://doi.org/10.1145/3359183

Monge Roffarello, A. & Russis, L. de (2022). Towards Understanding the Dark Patterns That Steal Our Attention. In S. Barbosa, C. Lampe, C. Appert & D. A. Shamma (Hrsg.), *CHI Conference on Human Factors in Computing Systems Extended Abstracts* (S. 1–7). ACM. https://doi.org/10.1145/3491101.3519829

Narayanan, A., Mathur, A., Chetty, M. & Kshirsagar, M. (2020). Dark Patterns: Past, Present, and Future. *Queue*, *18*(2), 67–92. https://doi.org/10.1145/3400899.3400901

Netherlands Authority for Consumers and Markets (15. März 2023). Guidelines on the protection of the online consumer. *ACM*. https://www.acm.nl/en/publications/information-for-companies/acm-guideline/guidelines-protection-online-consumer#principles

Nuseir, M. T. (2018). Impact of misleading/false advertisement to consumer behaviour. *Int. J. Economics and Business Research,*, *16*(4), 453–465.

Organisation für wirtschaftliche Zusammenarbeit und Entwicklung (2022). Dark commercial patterns. *OECD Digital Economy Papers*(336). https://doi.org/10.1787/44f5e846-en

Samuelson, W. & Zeckhauser, R. (1988). Status Quo Bias in Decision Making. *Journal of Risk and Uncertainty*, *1*(1), 7–59.

Shankar, A., Shetty, R. & Nath K, B. (2019). A Review on Phishing Attacks. *International Journal of Applied Engineering Research*, *14*(9), 2171–2175.

Spencer, S. B. (2020). The Problem of Online Manipulation. *U. Ill. L. Rev.*, *2020*(3), 959–1005.

Statista. (2022). *Daily time spent on social networking by internet users worldwide from 2012 to 2022*. https://www.statista.com/statistics/433871/daily-social-media-usage-worldwide/

Statista. (2023). *Number of users of selected social media platforms in Europe from 2017 to 2027, by platform*. https://www.statista.com/forecasts/1334334/social-media-users-europe-by-platform

Strange, A. (2015). *LinkedIn pays big after class action lawsuit over user emails*. https://mashable.com/archive/linkedin-class-action

Susser, D., Roessler, B. & Nissenbaum, H. (2019). Online Manipulation: Hidden Influences in a Digital World. *Georgetown Law Technology Review*, *4*(1), 1–45. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3306006

Thaler, R. H. (2018). Nudge, not sludge. *Science (New York, N.Y.)*, *361*(6401), 431. https://doi.org/10.1126/science.aau9241

Thaler, R. H. & Sunstein, C. R. (2020). *Nudge: Wie man kluge Entscheidungen anstößt* (C. Bausum, Übers.) (16. Aufl.). *Ullstein: Bd. 37366*. Ullstein.

Tversky, A. & Kahneman, D. (1974). Judgment under Uncertainty: Heuristics and Biases. *Science*, *185*(4157), 1124–1131.

User Experience Professionals' Association (2005). UPA Verhaltenskodex für Usability Fachleute. https://uxpa.org/wp-content/uploads/sites/9/2018/08/CoC_German.pdf

UXP2 Dark Patterns. (2023, 13. Mai). *The dark side of UX Design*. https://darkpatterns.uxp2.com

Weber, F. & Schäfer, H.-B. (2017). „Nudging“, ein Spross der Verhaltensökonomie: Überlegungen zum liberalen Paternalismus auf gesetzgeberischer Ebene. *Der Staat*, *56*(4), 561–592. https://www.jstor.org/stable/45106322

Wilkie, W. L., Mela, C. F. & Gundlach, G. T. (1998). Does “Bait and Switch” Really Benefit Consumers? *Marketing Science*, *17*(3), 273–282. https://doi.org/10.1287/mksc.17.3.273

Abbildungsverzeichnis