# Versteckte Beeinflussung: Deceptive Patterns in beliebten mobilen Applikationen

Caroline Labres
Fachhochschule St. Pölten
3100 St. Pölten, Österreich
it241502@fhstp.ac.at

## ABSTRACT

Manipulative Designstrategien, bekannt als Dark oder Deceptive Patterns, finden häufig Verwendung in digitalen Medien, um Nutzer*innen zu unbewussten Entscheidungen zu verleiten. Ziel des Artikels ist zu erforschen, inwiefern die verschiedenen Typen dieser Muster in bekannten mobilen Applikationen zum Einsatz kommen und welche Auswirkungen sie allgemein auf das Nutzungsverhalten haben. Die Ergebnisse zeigen, dass diese jedenfalls einen Einfluss auf die Nutzer*innen haben, die diese Strategien wiederum nicht erkennen. In der Praxis treten die verschiedenen Muster, zu denen Nagging, Obstruction, Sneaking, Interface Interference und Forced Action zählen, oft in Kombination miteinander auf. In den Bereichen Bildung, soziale Netzwerke und E-Commerce stößt man vor allem auf visuell hervorgehobene Optionen, zu denen Nutzer*innen tendieren sollen, oder Maßnahmen, die die Löschung des Accounts oder die Kündigung des Abonnements erschweren.

## 1 Einleitung

In der digitalen Welt von heute spielen mobile Anwendungen eine zentrale Rolle im Alltag vieler Menschen. Gleichzeitig wächst die Zahl an Strategien, die nicht darauf abzielen, den Nutzer*innen einen Mehrwert zu bieten, sondern sie gezielt zu täuschen oder zu manipulieren. Derartige manipulative Designstrategien werden als Deceptive Patterns (oder auch Dark Patterns) bezeichnet. Sie nutzen irreführende Gestaltungselemente, Verschleierung und psychologische Schwächen, um zu Entscheidungen zu verleiten, die im Interesse der Betreiber und nicht der Nutzer*innen sind (Brignull, 2023; Gray et al., 2018).

Ziel dieses Artikels ist aufzuzeigen, welche verschiedenen Deceptive Patterns existieren und wie diese in der Praxis verwendet werden, um so ein Bewusstsein für die versteckten Beeinflussungstechniken zu schaffen. Zunächst wird definiert, was Deceptive Patterns sind und welche verschiedenen Typen existieren, beispielsweise Roach Motel oder Forced Continuity. Anschließend werden die drei Apps Duolingo, Instagram und Amazon auf Grundlage von einschlägiger Literatur und eigenen Beobachtungen analysiert, um die Verbreitung solcher Muster in den Bereichen Bildung, soziale Netzwerke und E-Commerce zu beleuchten. Zuletzt werden die Wirkung und Erkennung von Deceptive Patterns angeschnitten.

## 2 Definition

2010 definierte Brignull (2023) den Begriff Dark Pattern. Darunter versteht man, dass Nutzer*innen durch bestimmte Tricks im User Interface zu Interaktionen und Handlungen bewegt werden, die nicht in ihrem Interesse sind. Beispielsweise werden sie zum Abschluss eines Abonnements verführt oder ihnen wird mehrmals die Möglichkeit von In-App-Käufen angeboten. (Brignull, 2023; Gray et al., 2018, S. 1). Nun empfindet Brignull diesen Begriff allerdings als veraltet und verwendet in seinen neuesten Werken stattdessen die Bezeichnung Deceptive Pattern (zu Deutsch trügerische Muster), welche eine Kurzform für Deceptive or Manipulative Pattern ist (Brignull, 2023).

## 3 Arten von Deceptive Patterns

In der Literatur tauchen mehrere Möglichkeiten auf, wie Dark Patterns kategorisiert werden können. Conti und Sobiesk (2010) gehen von elf Kategorien aus, darunter Verwirrung, Ablenkung, Verschleierung, Ausnutzung von Fehlern und Schock, während Brignull et al. (2023) auf ihrer Webseite 16 Arten aufzählen (Confirmshaming, Fake Scarcity, Fake urgency, Hard to cancel etc.). Gray et al. (2018) teilen Deceptive Patterns wiederum in fünf Kategorien ein: Nagging, Obstruction, Sneaking, Interface Interference und Forced Action. Diese Einteilung findet sich öfters in der Literatur und wird als aktuell bezeichnet, weshalb diese auch in diesem Artikel herangezogen wird.

### 3.1 Nagging

Beim Nagging wird der oder die Nutzer*in bei einer Interaktion einmal oder mehrmals durch eine andere Aufgabe unterbrochen, die nicht mit der Interaktion im Zusammenhang steht. Beispiele hierfür sind Pop-Ups oder ablenkende Audiosignale, wodurch die Aufmerksamkeit in eine andere Richtung gelenkt wird (Gray et al., 2018, S. 5).

### 3.2 Obstruction

Obstruction bedeutet, dass den Nutzer*innen die Durchführbarkeit einer Aufgabe oder Interaktion erschwert wird, um sie davon abzuhalten. Hierbei gibt es drei Unterkategorien (Gray et al., 2018, S. 5-6):

*3.2.1 Roach Motel (Kakerlakenfalle).* Es ist zwar leicht in eine Situation zu kommen, doch umso schwerer ist es hinauszugelangen. Zum Beispiel ist das Löschen eines Accounts im Vergleich zu dessen Erstellung viel schwieriger oder sogar unmöglich, weil zum Beispiel eine Telefonnummer angerufen werden muss.

*3.2.2 Price Comparison Prevention (Verhinderung von Preisvergleichen).* Dem oder der Nutzer*in wird der Preisvergleich von Dienstleistungen oder Produkten erschwert.

*3.2.3 Intermediate Currency (Zwischenwährung).* Hierbei wird mittels echten Geldes eine virtuelle Währung in der Applikation gekauft, die gegen Dienstleistungen oder Waren getauscht werden kann (z.B. In-App-Käufe). Den Nutzer*innen soll somit das Gefühl für den echten Geldwert genommen werden.

## 3.3 Sneaking

Oftmals werden den Nutzer*innen relevante Informationen verheimlicht, verschleiert oder erst verzögert mitgeteilt, sodass diese veranlasst werden, bestimmte Handlungen auszuführen, die sie mit vollem Wissensstand nicht durchführen würden. Beispielsweise treten unvorhergesehen Kosten auf oder unerwünschte Auswirkungen der Handlung machen sich im Nachhinein bemerkbar. Dies wird unter dem Begriff Sneaking zusammengefasst und dabei unterscheidet man vier verschiedene Arten (Gray et al., 2018, S. 6-7):

*3.3.1 Forced Continuity (Erzwungene Kontinuität).* Nach dem Ablaufdatum eines zeitlich begrenzten Diensts oder einer kostenlosen Testphase werden dem oder der Nutzer*in Kosten verrechnet. Es wird die Versäumnis ausgenutzt und davon ausgegangen, dass der Service weiterhin oder nun eine gebührenpflichtige Version genutzt werden möchte.

*3.3.2 Hidden Costs (Versteckte Kosten).* Hierbei werden bestimmte Kosten erst später offengelegt. Eine Dienstleistung oder Ware wird im ersten Moment mit einem speziellen Preis beworben, der sich durch hohe Versandkosten, eine zeitliche Begrenzung oder zusätzliche Gebühren dann allerdings erhöht.

*3.3.3 Sneak into Basket (In den Warenkorb schleichen).* Es werden Artikel in den Warenkorb gelegt, die dann unwissentlich von den Nutzer*innen gekauft werden. Argumentiert wird, dass die Artikel Vorschläge basierend auf den vorherigen Käufen sind.

*3.3.4 Bait and Switch (Lockvogeltaktik).* Auf eine bestimmte Handlung des oder der Nutzer*in folgt ein unvorhergesehenes und womöglich unerwünschtes Ereignis, welches nicht den Erwartungen entspricht. Beispielsweise wird beim Klick auf das rote „X“ nicht das Dialogfenster geschlossen, sondern die Webseite der Marke geöffnet.

## 3.4 Interface Interference

Unter Interface Interference versteht man jegliche Manipulation des User Interfaces (Benutzeroberfläche), sodass bestimmte Interaktionen wahrscheinlicher auftreten als andere. Dabei soll der oder die Nutzer*in verwirrt werden und die Auffindbarkeit von gewissen Interaktionsmöglichkeiten eingeschränkt werden. Diese Täuschungen lassen sich in drei Kategorien einteilen (Gray et al., 2018, S. 7-8):

*3.4.1 Hidden Information (Versteckte Informationen).* Den Nutzer*innen werden wichtige Handlungsmöglichkeiten verschwiegen, indem sie schwer oder nicht sofort zugänglich gemacht werden. Ziel ist, diese irrelevant erscheinen zu lassen. Die Informationen oder Optionen können sich beispielsweise im Kleingedruckten, in Form eines verfärbten Texts oder in den AGBs verstecken.

*3.4.2 Preselection (Vorauswahl).* Hierbei wird eine Option vorausgewählt, die aus der Sicht des Betreibers die gewünschte Wahl ist, jedoch nicht aus der Sicht der Nutzer*innen. Dadurch akzeptieren sie diese Standardoption eher, denn sie denken, dass in ihrem Interesse gehandelt wird.

*3.4.3 Aesthetic Manipulation (Ästhetische Manipulation).* Durch gewisse Designentscheidungen wird die Aufmerksamkeit der Nutzer*innen in eine bestimmte Richtung gelenkt, sodass sie davon überzeugt sind oder von anderen Informationen abgelenkt werden. Innerhalb dieser Kategorie gibt es vier genauere Unterteilungen (Gray et al., 2018, S. 7-8):

*3.4.3.1 Toying with Emotion (Spiel mit Gefühlen).* Der oder die Nutzer*in wird von einer Emotion, die durch Sprache, Farbe, Stil etc. hervorgerufen wird, zu einer Handlung oder Interaktion verleitet. Neben niedlichen Bildern oder einer beängstigenden Sprache kann auch ein Timer ein Auslöser sein, um Druck auszuüben.

*3.4.3.2 False Hierarchy (Falsche Hierarchie).* Hier wird die Auswahl einer Option durch Hervorhebung beeinflusst. Bei den Nutzer*innen soll das Gefühl entstehen, die beste oder einzige Wahl getroffen zu haben.

*3.4.3.3 Disguised Ad (Getarnte Werbung).* Anzeigen werden als Download-Button, interaktives Spiel oder auf eine andere Art und Weise getarnt.

*3.4.3.4 Trick Questions (Fangfragen).* Zu dieser Kategorie zählen Fragen, die auf den ersten Blick klar erscheinen, in Wirklichkeit aber eine andere Bedeutung haben. Dabei wird mit verwirrender Formulierung, Doppelverneinungen oder manipulativer Sprache gearbeitet.

## 3.5 Forced Action

Die letzte Kategorie an Deceptive Patterns umfasst Aktionen, die der oder die Nutzer*in ausführen muss, um den Zugriff zu speziellen Funktionen zu erhalten oder aufrechtzuerhalten. Diese können als letzter Schritt eines Vorgangs oder als vorteilhafte Option getarnt sein. Hierbei wird nochmal zwischen drei verschiedene Arten unterschieden (Gray et al., 2018, S. 8):

*3.5.1 Social Pyramid (Soziale Pyramide).* Der oder die Nutzer*in muss weitere Personen einladen, ebenfalls die Applikation zu nutzen, um Vorteile zu erhalten oder exklusive

Funktionen nutzen zu können. Häufig sieht man dieses Muster in Online-Spielen oder sozialen Medien.

*3.5.2 Privacy Zuckering.* Darunter fallen verwirrende Privatsphäre-Einstellungen, wodurch die Nutzer*innen mehr Informationen von sich preisgeben, als sie eigentlich möchten. Ein Beispiel dafür ist der in den AGBs oder Datenschutzrichtlinien verankerte Verkauf von Nutzerdaten an Dritte.

*3.5.3 Gamification.* Allgemein versteht man unter Gamification, dass Elemente aus Videospielen außerhalb des spielerischen Kontexts verwendet werden, um das Nutzungserlebnis zu verbessern (Deterding et al., 2011). Zu dieser Untergruppe von Deceptive Patterns zählen Situationen, in der sich wiederholende, meist unerwünschte Aufgaben erledigt werden müssen, um sich bestimmte Aspekte des Services zu verdienen. Oftmals können In-App-Käufe genutzt werden, um dies zu beschleunigen (Gray et al., 2018, S. 8).

## 4 Deceptive Patterns in mobilen Applikationen

Di Geronimo et al. (2020) untersuchten 240 kostenlose Apps aus den acht beliebtesten Kategorien aus dem Google Play Store, darunter Amazon, Netflix, Facebook und Spotify. Dabei fanden sie heraus, dass 95% der Apps mindestens ein Deceptive Pattern enthalten. Insgesamt wurden bei der Analyse 1.787 Deceptive Patterns gefunden, was bedeutet, dass eine App durchschnittlich sieben verschiedene Arten verwendet. Die häufigsten Strategien sind Nagging, False Hierarchy und Preselection (Di Geronimo et al., 2020). In den folgenden Unterkapiteln werden beispielhaft Apps aus drei Kategorien angeführt und beschrieben, wie diese Deceptive Patterns verwenden.

### 4.1 Duolingo – Bildung

Duolingo ist eine beliebte gamifizierte Sprachlern-App, bei der Vokabel und Grammatik in immer schwieriger werdenden Lektionen erlernt werden. Wird eine Frage falsch beantwortet, so verliert der oder die Nutzer*in ein Herz. Sind alle Herzen verbraucht, so muss er oder sie einen bestimmten Zeitraum abwarten oder kann durch In-App-Käufe die Herzen wieder auffüllen. Dabei wird eine virtuelle Währung namens „Gems“ verwendet, mit denen Power-Ups und Herzen erkauft werden können, sodass die Nutzer*innen das Gefühl für den tatsächlichen Geldwert verlieren (Intermediate Currency). Das Forced Action Deceptive Pattern zeigt sich durch die Möglichkeit, ein Werbevideo anzuschauen, um eine Truhe mit Gems zu erhalten (Peter, 2023). Wird die App für mindestens zehn Minuten verwendet, so fallen noch weitere Muster auf. Es werden wiederholt für mehrere Sekunden andauernde Werbevideos oder interaktive Anzeigen geschaltet (Nagging und Disguised Ad), wobei der oder die Nutzer*in bei einer Interaktion unerwarteterweise zum App Store geleitet wird (Bait and Switch). Außerdem kann ein kostenpflichtiges Abonnement („Super Duolingo“) abgeschlossen werden, welches keine Werbung, unbegrenzte Herzen und vieles mehr enthält. Dabei werden vor allem Deceptive Patterns aus der Kategorie Interface Interference genutzt (siehe Abbildung 1). Es wird das Jahres-Einzelabo vorselektiert (Preselection) und es scheint so, als gäbe es nur zwei Möglichkeiten. Hinter dem Button „Alle Abos anzeigen“ versteckt sich allerdings eine dritte Option, die monatlich gezahlt wird (Hidden Information). Allgemein findet man in der App oft visuell hervorgehobene Auswahlmöglichkeiten (siehe Abbildung 1), wodurch der oder die Nutzer*in zu bestimmten Aktionen gedrängt wird (Aesthetic Manipulation: Toying with Emotion und False Hierarchy). Was das Abonnement betrifft, so wird es nach der kostenlosen Testphase automatisch verlängert (Forced Continuity).

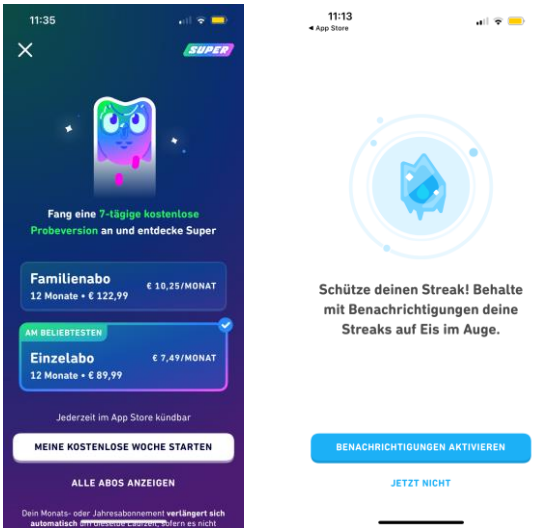


**Abbildung 1: Screenshots der App Duolingo, die Preselection, Hidden Information und Aesthetic Manipulation beinhalten**

### 4.2 Instagram – Soziale Netzwerke

In sozialen Netzwerken wie Instagram lassen sich mehrere Deceptive Patterns finden. Ein Account lässt sich leicht erstellen, die Funktion, diesen wieder zu löschen, ist allerdings versteckt. Diese Aktion wird den Nutzer*innen somit erschwert, was auf die Verwendung des Roach Motels hindeutet (Di Geronimo et al., 2020, S. 6). Oftmals wird bei Dialogfenstern eine von zwei Optionen hervorgehoben (z.B. der Button zum Erlauben des Zugriffs auf die Kontakte), was dem Interface Interference entspricht. Weiters wird das Privacy Zuckering angewendet (Mildner, Freye, et al., 2023, S. 2367). Laut Mildner, Savino et al. (2023) lassen sich alle fünf Arten aus Kapitel 3 in der App finden. Auch andere soziale Netzwerke wie Facebook, X und TikTok verwenden vor allem Deceptive Patterns wie Interface Interference, Obstruction und Privacy Zuckering (Mildner, Freye, et al., 2023, S. 2366).

### 4.3 Amazon – E-Commerce

Das Roach Motel Deceptive Pattern wird auch von der beliebten E-Commerce-Plattform Amazon genutzt. Die Kündigung einer Prime-Mitgliedschaft ist im Vergleich zu dessen Abschluss schwieriger aufzufinden und durchzuführen (Di Geronimo et al., 2020, S. 6). Weiters spielt Amazon mit den Gefühlen der Nutzer*innen, indem ihnen klargemacht wird, dass sie sofort alle Vorteile verlieren würden, und zählt diese erneut auf (Toying with

Emotion) (siehe Abbildung 2). Allgemein werden bestimmte Farben und Formulierungen genutzt, um die Nutzer*innen davon abzuhalten die Mitgliedschaft zu kündigen (Aesthetic Manipulation) (Verbraucherzentrale Bundesverband e.V., 2022, S. 2-3). Aesthetic Manipulation wird auch, wie bei vielen anderen Webseiten und Applikationen, im Cookie-Banner verwendet (siehe Abbildung 2).

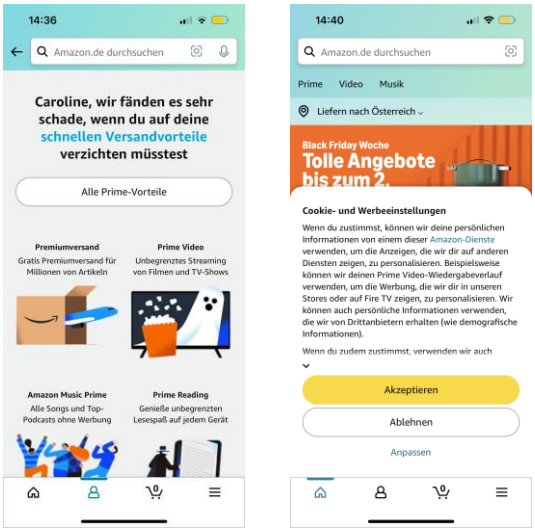


**Abbildung 2: Screenshots der App Amazon, die Toying with Emotion und False Hierarchy beinhalten**

## 5 Wirkung und Erkennung

Luguri und Strahilevitz (2021) erforschten die Wirkung von milden und aggressiven Deceptive Patterns. Die Ergebnisse zeigen, dass beide einen Einfluss auf das Verhalten der Nutzer*innen haben. Die Wahrscheinlichkeit, sich für einen bedenklichen Service zu registrieren, war in dem durchgeführten Experiment bei den Nutzer*innen, die mit milden Deceptive Patterns konfrontiert wurden, doppelt und bei denen, die aggressiven Deceptive Patterns ausgesetzt wurden, viermal so hoch wie bei der Kontrollgruppe. Die aggressiven Formen wurden allerdings auch als störender empfunden als die milderen. Zu den Deceptive Patterns, die am meisten Wirkung zeigten und die Nutzer*innen manipulierten bestimmte Entscheidungen zu treffen, die nicht in ihrem Interesse sind, zählen Hidden Information, Trick Questions und Obstruction. Di Geronimo et al. (2020) untersuchten mittels einer Online-Umfrage die Erkennung von fünf bzw. sechs Deceptive Patterns: Nagging, Intermediate Currency, Sneak into Basket in Kombination mit Preselection, False Hierarchy und Forced Action. Dabei stellten sie fest, dass Nutzer*innen diese Muster oft nicht erkennen, und sprechen deshalb von einer DP-Blindheit (DP-blindness).

## FAZIT

Es gibt viele verschiedene Arten von Deceptive Patterns, die häufig in mobilen Applikationen zum Einsatz kommen. 95% der Apps im Google Play Store nutzen mindestens eines dieser Muster. Diese können in fünf Kategorien eingeteilt werden, nämlich Nagging, Obstruction, Sneaking, Interface Interference und Forced Action. Viele davon finden auch in den Bereichen Bildung, soziale Netzwerke und E-Commerce Verwendung. In der gamifizierten Sprachlern-App Duolingo findet man beispielsweise In-App-Käufe mit einer eigenen virtuellen Währung, freiwillige und unfreiwillige Werbe-Unterbrechungen und visuell hervorgehobene Buttons. Bei der Bewerbung des kostenpflichtigen Abonnements wird wiederum eine Option vorselektiert und andere versteckt. Sowohl hier als auch bei Amazon wird das Abo bzw. die Mitgliedschaft nach Ablauf verlängert, was den Betreibern zugutekommt. Die Kündigung der Mitgliedschaft bzw. die Löschung des Accounts wird den Nutzer*innen auf Plattformen wie Amazon oder Instagram ebenso erschwert. Allgemein kann gesagt werden, dass viele der Deceptive Patterns in gewissen Kombinationen auftreten und dass vor allem oft Aesthetic Manipulation genutzt wird, genauer gesagt Toying with Emotion und False Hierarchy. Während die einen Deceptive Patterns als störend empfunden werden, fallen andere den Nutzer*innen gar nicht auf. Jedenfalls haben sie einen gewissen Einfluss auf ihre Handlungsentscheidungen, weshalb es umso interessanter ist, spezifische Apps hinsichtlich der Verwendung und Wirkung solcher Muster noch genauer zu untersuchen. Hinzu kommen Fragen nach ethischen Grundsetzen und der Erkennung solcher Muster, mit denen man sich beschäftigen muss, wenn die Häufigkeit von Deceptive Patterns in Zukunft weiter zunimmt.

## LITERATUR


Brignull, H. (2023). *Deceptive Patterns: Exposing the Tricks Tech Companies Use to Control You*. Testimonium Ltd.

Brignull, H., Leiser, M., Santos, C., & Doshi, K. (2023, 25. April). *Deceptive patterns – user interfaces designed to trick you*. https://www.deceptive.design/ (Abgerufen am 23.11.2024)

Conti, G., & Sobiesk, E. (2010). Malicious interface design: Exploiting the user. *Proceedings of the 19th international conference on World wide web*, 271–280. https://doi.org/10.1145/1772690.1772719

Deterding, S., Dixon, D., Khaled, R., & Nacke, L. (2011). From game design elements to gamefulness: Defining „gamification". *Proceedings of the 15th International Academic MindTrek Conference: Envisioning Future Media Environments*, 9–15. https://doi.org/10.1145/2181037.2181040

Di Geronimo, L., Braz, L., Fregnan, E., Palomba, F., & Bacchelli, A. (2020). UI Dark Patterns and Where to Find Them: A Study on Mobile Applications and User Perception. *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*, 1–14. https://doi.org/10.1145/3313831.3376600

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

Luguri, J., & Strahilevitz, L. J. (2021). Shining a Light on Dark Patterns. *Journal of Legal Analysis*, *13*(1), 43–109. https://doi.org/10.1093/jla/laaa006

Mildner, T., Freye, M., Savino, G.-L., Doyle, P. R., Cowan, B. R., & Malaka, R. (2023). Defending Against the Dark Arts: Recognising Dark Patterns in Social Media. *Proceedings of the 2023 ACM Designing Interactive Systems Conference*, 2362–2374. https://doi.org/10.1145/3563657.3595964

Mildner, T., Savino, G.-L., Doyle, P. R., Cowan, B. R., & Malaka, R. (2023). About Engaging and Governing Strategies: A Thematic Analysis of Dark Patterns in Social Networking Services. *Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems*, 1–15. https://doi.org/10.1145/3544548.3580695

Peter, M. (2023, 6. Februar). Dark Patterns in Popular Mobile Apps. *Medium*. https://medium.com/@marcpeter1997/dark-patterns-in-popular-mobile-apps-296011029579

Verbraucherzentrale Bundesverband e.V. (2022). *Dark Patterns—Manipulatives Design im Internet: Fallsammlung aus dem Verbraucheraufruf „Dark Patterns" der Marktbeobachtung Digitales (Stand: 09.02.2022)*. https://www.edpb.europa.eu/system/files/2022-05/2021-02-09_fallsammlung_verbraucheraufruf_dark_patterns.pdf