Masterarbeit

DARK PATTERNS – NUR FÜR MANCHE DUNKEL?

Untersuchung Digitaler Kompetenz als Einflussfaktor auf die Wirkung von Dark Patterns

Larissa Mörgeli
14-6303-62
[redacted]

Zürich, 16. Juni 2022

Betreuung: Dr. Marcus Zimmer
Ko-Betreuung: Carmen Oswald

Master of Science in Business Administration with a Specialization in Marketing
Schriftliche Arbeit verfasst an der School of Management and Law,
Zürcher Hochschule für Angewandte Wissenschaften

Management Summary

Onlinedienste arbeiten kontinuierlich daran, ihre Leistungskennzahlen zu verbessern. Dabei ist der Einsatz von manipulativen Praktiken weit verbreitet. Vermehrt werden Dark Patterns – eine Form der Manipulation, bei der Erkenntnisse aus der Psychologie im Design von Nutzeroberflächen einsetzt werden, mit dem Ziel die Nutzenden zu einem Verhalten zu verleiten, das deren eigenen Interessen entgegenstrebt – angewendet. Dark Patterns sind grossteils mit negativen Konsequenzen für die Konsument_innen verbunden und erste Erkenntnisse aus der Forschung weisen darauf hin, das nutzergruppenspezifische Faktoren wie der Bildungsstand und das Alter die Wirkung von Dark Patterns beeinflussen. Die Identifikation von Faktoren, die zur Vulnerabilität der Konsument_innen beitragen, ist insbesondere im Rahmen des Konsumentenschutzes von Relevanz und bedarf weiterführender empirischer Forschung.

Diese Arbeit nimmt sich dieser Forschungslücke an und untersucht Einflüsse auf die Wirkung von Dark Patterns anhand der Anwendung von Dark Patterns auf Cookie-Zustimmungshinweisen. Aufbauend auf bestehender Forschung wird untersucht, ob die Digitale Kompetenz der Nutzenden einen Einfluss auf die Erkennung von Dark Patterns, sowie deren Wirkung hat und ob die Wirkung von Dark Patterns durch deren Erkennung abgeschwächt wird.

Dazu wurde ein Laborexperiment durchgeführt, in dessen Rahmen die Digitale Kompetenz der Proband_innen erhoben wurde. Einleitend zur Befragung wurde ein Cookie-Zustimmungshinweis präsentiert, welcher experimentell manipuliert wurde. Im Cookie-Zustimmungshinweis der Experimentalgruppe wurde ein Set an Dark Patterns eingesetzt, während der Hinweis der Kontrollgruppe frei von manipulativen Elementen gestaltet wurde.

Die Analyse des Zusammenhangs zwischen dem Einsatz von Dark Patterns zur Manipulation hinsichtlich der Zustimmung zu den Cookies, ergab keine signifikanten Effekte. Die Hinweise wurden bereits ohne den Einsatz von Dark Patterns mit 82.1 Prozent mehrheitlich akzeptiert, wobei die Zustimmung unter Einsatz von Dark Patterns

um 9.0 Prozent höher lag. Weiter wurden keine Effekte der Digitalen Kompetenz auf die Zustimmung zu den Cookies oder auf die Wirkung der Dark Patterns festgestellt. Das Messkonstrukt der Erkennung von Dark Patterns wies Schwächen im Bereich der Inhaltsvalidität auf und stand in keinem Zusammenhang zur Wirkung der Dark Patterns. Die in dieser Arbeit aufgestellten Hypothesen wurden somit allesamt abgelehnt.

Das Ausbleiben des direkten Effekts von Dark Patterns auf die Zustimmung zu den Cookies könnte damit begründet werden, dass aufgrund der Allgegenwärtigkeit von manipulativen Praktiken auf Cookie-Hinweisen eine Konditionierung der Konsument_innen erfolgte, wodurch unabhängig von deren Ausgestaltung, diese akzeptiert werden. Weiter wird darauf hingewiesen, dass die Untersuchung anhand des Anwendungsfalls der Cookie-Zustimmungshinweise einige anwendungsspezifische Besonderheiten aufweist, welche die Generalisierbarkeit einschränken. Aus diesem Grund wird eine Wiederholung der Untersuchung des Einflusses der Digitalen Kompetenz auf die Wirkung von Dark Patterns anhand eines anderen Einsatzgebietes von Dark Patterns, empfohlen.

Inhaltsverzeichnis

Abbildungsverzeichnis

Tabellenverzeichnis

Abkürzungsverzeichnis

EU	Europäische Union
DSGVO	Datenschutz-Grundverordnung
etc.	et cetera

1 Einleitung

Dieses Kapitel erläutert die Ausgangslage der Thematik, zeigt die Problemstellung und Forschungslücke auf, und beschreibt die Forschungsfragen und Zielsetzung der Arbeit. Anschliessend wird die Arbeit abgegrenzt, sowie deren Aufbau erklärt.

1.1 Ausgangslage

Die Disziplin der Entscheidungsarchitektur beschäftigt sich mit der Art und Weise wie den Konsument_innen Auswahlmöglichkeiten präsentiert werden und wie die Entscheidungsfindung dadurch beeinflusst werden kann (Thaler & Sunstein, 2009, S. 81). Viel thematisiert ist die Praktik des Nudgings, bei der das Verhalten von Menschen in vorhersehbarer Weise beeinflusst wird, ohne Optionen zu verbieten oder wirtschaftliche Anreize einzusetzen (Thaler & Sunstein, 2009, S. 6). «Digitales Nudging», respektive Nudging in digitalen Umgebungen, welches mittels User Interface Design beabsichtigt, das Verhalten der Nutzer_innen von Onlinediensten in eine bestimmte Richtung zu lenken, steht allerdings unter kritischer Beobachtung (Reisch, 2020, S. 87). Kritisiert wird insbesondere, dass psychologische Schwachstellen der Nutzer_innen zu Gunsten des Anbieters ausgenutzt werden, statt Bedingungen zu schaffen, die für beide Parteien vorteilig sind (Burr et al., 2018, S. 748). So konnte beispielsweise aufgezeigt werden, dass digitale Nudges Impulskäufe fördern (Moser et al., 2019, S. 1). Deshalb wurden Leitfäden wie beispielsweise das FORGOOD Framework von Lades und Delaney (2022, S. 77) entwickelt, um Entwickler_innen von solchen Nudges hinsichtlich ethischer Abwägungen zu unterstützen und eine Art Regelwerk für den Einsatz von digitalem Nudging zu schaffen.

Eine Methodik zur Verhaltenssteuerung auf Online-Diensten, die ethischen Grundsätzen widerspricht, sind «Dark Patterns» (Bogenstahl, 2019, S. 1). Der Begriff Dark Patterns beschreibt Designpraktiken, die darauf ausgelegt sind, Nutzer_innen von Onlinediensten zu einem Verhalten zu bewegen, welches deren Interessen entgegenläuft und mit negativen Konsequenzen für die Nutzer_innen verbunden sein kann (Brignull, 2010c). Dark Patterns sind Studien zufolge sehr weit verbreitet, finden verschiedene

Anwendungsformen und sind demnach für Nutzer_innen von digitalen Diensten von grosser Bedeutung (Di Geronimo et al., 2020, S. 1; Mathur et al., 2019, S. 27).

1.2 Problemstellung und Forschungslücke

Im Bereich von Dark Patterns liegt insgesamt noch wenig Forschung vor. Eine erste Welle der akademischen Forschung widmete sich der Identifikation, Typologisierung und Quantifizierung von Dark Patterns (Bösch et al., 2016; Brignull, 2010a ; Di Geronimo et al., 2020). Ergänzend dazu wurden Studien zur Messung Effekte von Dark Patterns in verschiedenen Kontexten durchgeführt (Luguri & Strahilevitz, 2019; Nouwens et al., 2020; Sin et al., 2022). Dabei wurden Unterschiede in den Effekten von Dark Patterns, bezugnehmend auf den Bildungsgrad (Bongard-Blanchy et al., 2021, S. 774; Luguri & Strahilevitz, 2019, S. 1) und das Alter (Bongard-Blanchy et al., 2021, S. 774) der Nutzer_innen festgestellt, was weitergehende nutzerspezifische Einflüsse auf die Wirkungsweise von Dark Patterns vermuten lässt. Entsprechende Studien zu nutzerspezifischen Faktoren, welche die Wirkung von Dark Patterns moderieren, liegen allerdings noch nicht vor.

1.3 Zielsetzung

Die Arbeit nimmt sich dieser Forschungslücke an und hat das Ziel einen Beitrag zur Erforschung nutzerspezifischer Wirkungsunterschiede von Dark Patterns zu liefern. Die Arbeit soll auf den Beobachtungen von Bongard-Blanchy et al. (2021) und Luguri & Strahilevitz (2019) zu Wirkungsunterschieden in Bezug auf den Bildungsgrad und das Alter aufbauen und diese erweitern. Erkenntnisse zu Unterschieden hinsichtlich der Anfälligkeit für Dark Patterns und damit die Identifikation besonders schützenswerter Nutzergruppen sind insbesondere für die Entwicklung und den Ausbau von Konsumentenschutzmassnahmen in Bezug auf Dark Patterns von Relevanz.

1.4 Forschungsfragen

Bezugnehmend auf die Zielsetzung sollen im Rahmen der Arbeit die folgenden Forschungsfragen beantwortet werden:

1. Sind Nutzer_innen, die eine höhere Digitale Kompetenz aufweisen, eher in der Lage, Dark Patterns zu erkennen?
2. Wird die Wirkung von Dark Patterns durch die Fähigkeit, diese zu erkennen, abgeschwächt?
3. Wird die Wirkung von Dark Patterns durch eine höhere Digitale Kompetenz der Nutzer_innen, abgeschwächt?

1.5 Abgrenzung

An dieser Stelle wird das Thema inhaltlich abgegrenzt, um zu erläutern, welche Punkte im Rahmen der Arbeit nicht behandelt werden.

Während die meisten Definitionen Dark Patterns als Praktiken im Design von Digitalen Medien eingrenzen (Brignull, 2010b; Mathur, 2021, S. 2) , wird der Begriff teilweise auch im Bereich architektonischer Designs oder anderer Offlineaspekten angewendet (Baroni et al., 2021, S. 2; Chivukula et al., 2019, S. 5). Letzteres ist allerdings eher im etwas breit gefassteren Begriff «Sludging» einzuordnen (Sunstein, 2020, S. 4). In dieser Arbeit werden jedoch nur Einsatzgebiete von manipulativen Designpraktiken betrachtet, welche das Interfacedesign betreffen und damit der weiter verbreiteten Definition von Dark Patterns entsprechen. Weiter werden klassische Cyberkriminalitäts-Techniken nicht detailliert thematisiert.

Die vorliegende Arbeit argumentiert vorwiegend aus Konsumentensicht und thematisiert Aspekte des Konsumentenschutzes. Vorteile, welche sich für Onlinedienste durch den Einsatz von Dark Patterns ergeben könnten, werden weniger stark beleuchtet.

1.6 Vorgehensweise und Aufbau

Die Arbeit ist in fünf Teile gegliedert. Im anschliessenden Kapitel soll der theoretische Hintergrund zur Verhaltensökonomie und Entscheidungsarchitektur, sowie der aktuelle Forschungsstand zum Thema Dark Patterns erörtert werden.
Im dritten Kapitel wird das methodische Vorgehen erläutert. Aufbauend auf dem konzeptionellen Modell werden die Variablen operationalisiert und der Aufbau des Experiments wird beschrieben.

Das vierte Kapitel widmet sich der Auswertung des Experiments und den Resultaten. Im letzten Kapitel werden die Resultate, sowie das Vorgehen kritisch diskutiert, sowie in Bezug zur bestehenden Literatur gesetzt. Abschliessend werden Limitationen der Arbeit aufgezeigt und Implikationen für Theorie und Praxis genannt, und es wird auf weiteren Forschungsbedarf eingegangen.

2 Stand des Wissens

Im folgenden Kapitel wird der wissenschaftliche Forschungsstand zu mit der Forschungsfrage verwandten Themen aufgearbeitet. Zu Beginn wird ein kurzer Überblick über die Verhaltensökonomik und Entscheidungsarchitektur geschaffen, um die Dark-Pattern-Thematik im entsprechenden Kontext einzuordnen. Anschliessend wird der aktuelle Forschungsstand zu Dark Patterns und die damit einhergehende Konsumentengefährdung vertieft erläutert. Abschliessend wird das Konzept der Digitalen Kompetenz ausgeführt und deren mögliche Bedeutung in Zusammenhang mit Dark Patterns diskutiert.

2.1 Verhaltensökonomik

Die traditionelle Wirtschaftstheorie postuliert den Menschen als wirtschaftliches und rational agierendes Wesen (Simon, 1955, S. 241). Gemäss der Theorie des «homo oeconomicus» agiert der Mensch unter unbegrenzter Rationalität, unbegrenzter Willenskraft und unbegrenztem Eigennutzstreben und trifft demnach Entscheidungen nach dem Optimumprinzip (Beck, 2014, S. 2). In der Beobachtung des tatsächlichen Verhaltens zeigt sich allerdings, dass dieses häufig dem Prinzip der Rationalität oder der subjektiven Nutzenmaximierung widerspricht (Hargreaves Heap, 2013, S. 985). Der Untersuchung ebendieser Anomalien widmet sich die Disziplin der Verhaltensökonomik (behavioural economics) (Brzezicka & Wisniewski, 2014, S. 356). Dabei stützt sich die Wissenschaft der Verhaltensökonomik auf Hypothesen aus der Psychologie, um ökonomische Entscheidungsverhalten der Menschen zu erklären (Beck, 2014, S. 9; Brzezicka & Wisniewski, 2014, S. 354).

Herbert A. Simon (1955, S. 251) führte den Begriff der unvollkommenen Rationalität (bounded rationality) ein, der beschreibt, dass Entscheidungen, entgegen der Annahme der traditionellen Wirtschaftstheorie, nicht nach dem Prinzip der Nutzenmaximierung, sondern dem Anspruchserfüllung (satisficing) gefällt werden (Kahneman, 2003, S. 1449). In vielen Situationen fehlen den Menschen die Zeit, die Willenskraft oder die kognitiven Ressourcen, um rational und logisch zu handeln, weshalb für die Entscheidungsfindung auf vereinfachende Regeln, sogenannte Heuristiken, zurückgegriffen wird (Beck, 2014,

S. 26; Marchiori et al., 2017, S. 3). Das Wort «Heuristiken» stammt vom griechischen «heuriskein» ab und bedeutet so viel wie «verbesserte Problemlösung» und kann ebenfalls als «Daumenregel» verstanden werden (Beck, 2014, S. 25–26). Heuristiken sind nützlich, indem sie uns dabei unterstützen, ein Problem schneller zu lösen, können allerdings auch zu systematischen Fehlern und zu Verzerrungen (biases) führen (Tversky & Kahneman, 1974, S. 1124). Die Untersuchung des Lösungsfindungsprozess wurde stark durch die Forschung von Tversky und Kahneman (1974) geprägt, welche die drei Heuristiken Repräsentativitätsheuristik, Verfügbarkeitsheuristik und Verankerungs-heuristik identifizierten (Beck, 2014, S. 26).

Ein Ansatz zur Erklärung, weshalb der Mensch auf solche Heuristiken zurückgreift, lieferte Kahnemans Theorie des Denkens mittels zwei Systemen (Kahneman, 2011). Demnach funktioniert das System 1 automatisch, schnell und unbewusst und das System 2 wird für bewusste und aufwändige Denkprozesse eingesetzt (Kahneman, 2011, S. 33). Die meisten Entscheidungen werden über das System 1 gefällt, was den Einsatz von Heuristiken und das Auftreten von Verzerrungen begünstigt (Stanovich & West, 2000, S. 658).

2.2 Entscheidungsarchitektur

Der Begriff der Entscheidungsarchitektur (choice architecture) wurde durch die Forscher Thaler und Sunstein (2009, S. 81) eingeführt und beschreibt, wie Erkenntnisse aus der Verhaltensökonomik genutzt werden können, um das Verhalten von Menschen zu beeinflussen. Ein zentraler Begriff in der Entscheidungsarchitektur ist «Nudging». Thaler und Sunstein (2009, S. 6) definierten Nudging als Massnahmen, die Auswahlarchitekten einsetzen, um das Verhalten von Menschen in vorhersehbarer Weise zu beeinflussen, ohne Optionen zu verbieten oder wirtschaftliche Anreize einzusetzen. Nudges können beispielsweise mittels Formulierungen oder Darstellung geschaffen werden und beeinflussen den nicht-rationalen Agenten, der intuitiv handelt (System 1), nicht aber den rationalen Agenten (Hargreaves Heap, 2013, S. 993). Als Beispiel für einen Anwendungsfall von Nudging kann die automatische Erneuerung eines Abonnements genannt werden (Thaler & Sunstein, 2009, S. 35). Dieses Anwendungsbeispiel lässt sich

als «Default-Nudge» bezeichnen und nutzt aus, dass Menschen gerne an aktuellen Gegebenheiten festhalten (Status-quo-Verzerrung) (Thaler & Sunstein, 2009, S. 34).

Nudging basiert auf dem Prinzip des liberalen Paternalismus (Thaler & Sunstein, 2009, S. 5). «Liberal» beschreibt dabei, dass Entscheidungsfreiheit gewährleistet ist und «Paternalismus» steht für das Bestreben das Wohlergehen der Menschen zu steigern, indem das Verhalten in die entsprechender Richtung zu steuern versucht wird (Schmidt, 2017, S. 405). Nudges werden aber häufig dafür kritisiert, dass sie aufgrund ihres unterschwelligen Charakters die Autonomie der Individuen einschränken (Marchiori et al., 2017, S. 6). Kritiker_innen bringen an, dass Nudging Menschen in Richtungen manipuliert, die ihnen unbekannt sind und dass Nudges damit unethisch seien (Marchiori et al., 2017, S. 5).

Entgegen dem Prinzip der liberalen Paternalismus agieren nicht alle Verhaltensarchitekten im Interesse der Konsument_innen (Sunstein, 2020, S. 7). Sunstein (2020, S. 4) definiert Sludging als den Einsatz übermässiger Hürden, die es den Konsument_innen erschweren, ihre Interessen umzusetzen, wie beispielsweise die Bedingung, dass ein Abonnement nur mittels eines kostenpflichtigen Telefonanrufs gekündigt werden kann. In seinen Ausführungen zu Sludges weist Sunstein (2020, S. 5) allerdings gleichzeitig darauf hin, dass solche Hürden nicht zwingend als Sludge klassifiziert werden müssen, wenn sie beispielsweise dazu eingesetzt werden, den Konsument_innen Bedenkzeit zu bieten, um Fehler oder Leichtsinn zu vermeiden.

Heute findet ein Grossteil der Kaufentscheidungen online – via Desktop oder dem Mobilegerät – statt (Johnson et al., 2012, S. 491). Deshalb gewinnt die Thematik der Entscheidungsarchitektur im Onlineumfeld zunehmend an Relevanz (Mirsch et al., 2017, S. 635). Ausserdem sind Konsument_innen, aufgrund der Unmenge an Informationen im Internet und der damit einhergehenden kognitiven Überforderung, besonders anfällig für verhaltenssteuernde Massnahmen wie Nudging (Mirsch et al., 2017, S. 635; Murray et al., 2010, S. 232). Das Onlineumfeld bietet die Möglichkeiten, Nudging-Experimente kostengünstig und schnell umzusetzen und ermöglicht die Personalisierung der Nudges auf die Konsument_innen, was deren Effektivität steigern kann (Weinmann et al., 2016,

S. 5). Weiter sind auch technologiegestützte Hilfsmittel wie Suchmaschinen oder Produktempfehlungssysteme zu betrachten, welche die Entscheidungsfindung vereinfachen, aber auch steuern und manipulieren können (Häubl & Murray, 2005, S. 11). Werden Erkenntnisse des menschlichen Verhaltens im User Interface Design von beispielsweise Websites und Webshops eingesetzt, um die Konsument_innen zu unbeabsichtigten und potenziell schädlichen Entscheidungen zu zwingen, lenken oder täuschen, ist dieses Vorgehen im Bereich der Dark Patterns einzuordnen (Mathur et al., 2019, S. 2). Mögliche negative Konsequenzen sind beispielsweise Frustration, finanzielle Verluste oder das unbeabsichtigte Teilen von personenbezogenen Daten (Maier & Harr, 2020, S. 180). Die Thematik der Dark Patterns wird im folgenden Kapitel genauer ausgeführt.

2.3 Dark Patterns

Der Begriff «Dark Patterns» wurde erstmalig im Jahr 2010 von Harry Brignull (2010b) auf dessen Website darkpatterns.org (heute erreichbar unter: deceptive.design) erwähnt. Brignull (2010b) definierte Dark Patterns als Tricks, die auf Websites und in Apps eingesetzt werden, um Nutzer_innen dazu zu verleiten, Dinge zu tun, die sie nicht beabsichtigt hatten, wie zum Beispiel etwas zu kaufen oder sich für etwas anzumelden.

Dark-Pattern-Designer stützen sich bei ihrer Arbeit auf Erkenntnisse zu menschlichen Verhaltens- und Wahrnehmungsmustern aus der Verhaltensökonomik, welche im Kapitel 2.1 erläutert wurde (Bogenstahl, 2019, S. 1). Dark Patterns lassen sich im Bereich der Sludges einordnen, da sie Heuristiken und Verzerrung einsetzen, um die Konsument_innen zu täuschen oder zu manipulieren (Gunawan et al., 2021, S. 3; Thaler, 2018). Dabei wird das unbeabsichtigte und für die Konsument_innen allfällig schädliche Verhalten mittels nötigendem, lenkendem oder täuschendem Design der Nutzeroberfläche hervorgerufen (Mathur et al., 2019, S. 1).

Eines der am häufigsten eingesetzten Dark Patterns ist «False Hierarchy» (Di Geronimo et al., 2020, S. 5), welches in der Abbildung 1 anhand eines Beispiels illustriert wird. Im abgebildeten Beispiel wird die kostenpflichtige Sitzplatzwahl mittels eines farblich auffälligen und prominenten Buttons abgebildet, während die für die Konsument_innen

kostenfreie Option des Verzichts auf eine Sitzplatzwahl unauffällig mittels Textlink präsentiert wird. Die unauffällige Präsentation der kostenfreien Option wird erwartungsweise dazu führen, dass ein Grossteil der Jetstar-Kund_innen einen kostenpflichtigen Sitzplatz reserviert, ohne dies explizit gewollt zu haben, und damit Jetstars Umsatz steigert (Brignull, 2010a).

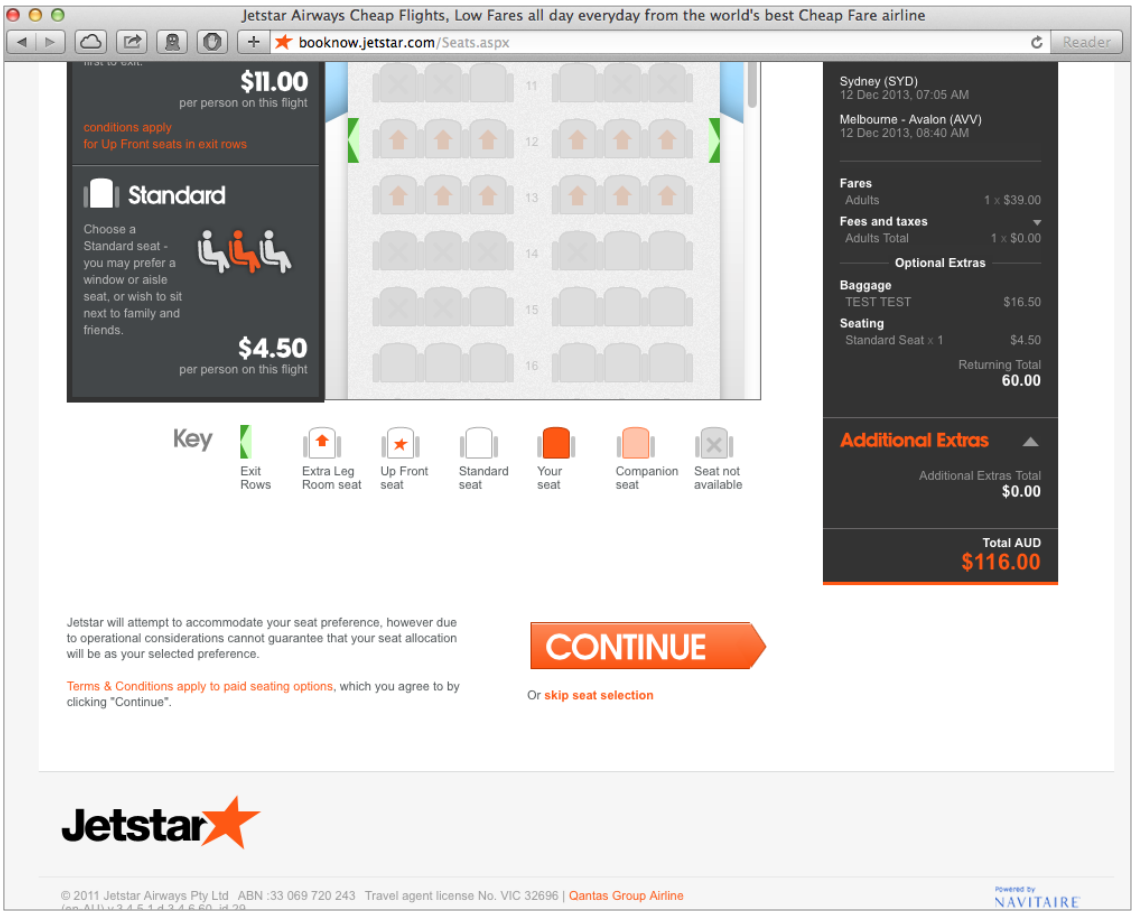


Abbildung 1: Beispiel «False Hierarchy» Dark Pattern (Brignull, 2010)

Dark Patterns sind sehr wirkungsvoll hinsichtlich gesetzten Zielen der Unternehmung wie beispielsweise der Verkaufssteigerung, können allerdings negative Effekte auf die Kundenzufriedenheit hervorrufen (Maier & Harr, 2020, S. 179).

Der Begriff «Dark Patterns» leitet sich vom Begriff der «Design Patterns» ab, was ein Konzept beschreibt, bei dem Problemlösungsansätze von einem spezifischen Anwendungsfall abstrahiert und verallgemeinert werden, sodass sie in verschiedenen,

passenden Szenarien angewendet werden können, was entsprechend auch auf Dark Patterns zutrifft (Bösch et al., 2016, S. 238).

An dieser Stelle ist anzumerken, dass eine starke Varietät an Definitionen von Dark Patterns vorherrscht und es teilweise an Präzision bei den entsprechenden Definitionen mangelt (Mathur et al., 2021, S. 7). In der Bestrebung das Verständnis für Dark Patterns zu schärfen, wurden verschiedenste Taxonomien erarbeitet und systematisch ergänzt (Luguri & Strahilevitz, 2019, S. 3; Mathur et al., 2019, S. 4). Einige der Taxonomien werden im nachfolgenden Kapitel vorgestellt und anschliessend wird eine Taxonomie ausgewählt, auf welche sich die weiterführenden Kapitel stützen.

2.3.1 Taxonomie

Die erste Dark-Pattern-Taxonomie stammte von Brignull (2010b) und umfasste 12 Dark Pattern-Typen. Ein Typus, der aus dieser initialen Taxonomie stammt, ist beispielsweise «Sneak into basket», wobei den Konsument_innen während des Kaufprozesses heimlich ein zusätzlicher, ungewollter Artikel in den Warenkorb gelegt wird (Brignull, 2010b).

Weitere Forschende entwickelten die Taxonomien anhand verschiedener Anwendungsfälle wie Video Games (Zagal et al., 2013), Mobile Apps (Lewis, 2014) oder Heimrobotersystemen (Lacey & Caudwell, 2019). In letzterem Anwendungsfall wurde beispielsweise ein niedliches Design von Heimrobotern als Dark Pattern klassifiziert, da es mitunter die Nutzer_innen dazu verleitet, unbewusstes Handeln bewusstem Denken vorzuziehen (Lacey & Caudwell, 2019, S. 379).

Ein weiterer Forschungszweig fokussierte sich auf «Privacy Dark Patterns», die eingesetzt werden, um die Sammlung personenbezogener Daten von Nutzer_innen auszuweiten (Bösch et al., 2016, S. 243). Ein wichtiger Begriff stellt in diesem Kontext «Privacy Zuckering» – benannt nach dem Facebook-CEO Mark Zuckerberg – dar (Brignull, 2010b). Privacy Zuckering beschreibt, dass die User mittels Designpraktiken entmutigt werden, Änderungen an den Privatsphäre Einstellungen vorzunehmen und die Sammlung personenbezogener Daten einzuschränken (Bösch et al., 2016, S. 248). Bösch et al. (2016, S. 252) nannten sieben Dark-Pattern-Typen, die im Zusammenhang mit der

Privatsphäre-Thematik häufig zum Einsatz kommen. «Unsterbliche Konten» beispielsweise führen dazu, dass den User_innen die Löschung des Accounts und der zugehörigen Daten erschwert oder sogar verunmöglicht wird (Bösch et al., 2016, S. 250). Generischer ist die Taxonomie von Gray et al. (2018, S. 5) gehalten, welche die fünf Kategorien «Nagging», «Obstruction», «Sneaking», «Interface Interference» und «Forced Action» formulierten und auf Basis derer ebenfalls die Auftretenshäufigkeit verschiedener Dark Patterns zu quantifizieren versucht wurde (Di Geronimo et al., 2020).

Mit dem Kritikpunkt, dass die verschiedenen Taxonomien auf Basis inkonsistenter oder unklarer Auslegungen von Dark Patterns erstellt wurden, unternahmen Luguri & Strahilevitz (2019, S. 9), sowie Mathur et al. (2021, S. 5) Bestrebungen, eine Übersicht über entstandene Taxonomien zu schaffen. Luguri & Strahilevitz (2019, S. 11) nahmen dabei eine Bereinigung der konsolidierten Taxonomien vor und berücksichtigten nur Techniken, die User_innen zu einem Verhalten manipulierten, welches deren Interessen entgegenläuft. Damit wurde beispielsweise das vorab genannte Beispiel der «Niedlichkeit» bei Heimrobotern ausgeschlossen, da dies das genannte Kriterium nicht erfüllte (Luguri & Strahilevitz, 2019, S. 11).

Im der folgenden Tabelle 1 werden in kurzer Form die revidierten Kategorien von Luguri & Strahilevitz (2019) wiedergegeben. Diese wurden als Basis für die Masterarbeit genutzt.

Tabelle 1: Dark-Pattern-Taxonomie (in Anlehnung an Luguri & Strahilevitz, 2019, S. 12)

Kategorie	Beschrieb
Nagging	Wiederholter Unterbruch der User Journey, beispielsweise mittels Pop-ups, mit der Aufforderung eine durch das Unternehmen gewünschte Aktion auszuüben (Gray et al., 2018, S. 5).
Social Proof	Ausnutzung des Nachahmungseffekts, durch beispielsweise irreführende oder gefälschte Aktivitätsmeldungen (z.B. «50 andere Kunden schauen sich dieses Produkt gerade an»)(Mathur et al., 2019, S. 18).

Obstruction	Unnötige Erschwerung einer gewünschten Aktion der Kund_innen, da vom Unternehmen nicht erwünscht (Gray et al., 2018, S. 5). Ein Beispiel für eine solche Taktik wäre, dass die Anmeldung zu einem Dienst für die User_innen sehr einfach gestaltet wird, die Abmeldung davon aber erschwert oder verunmöglicht wird, was Brignull (Brignull, 2010b) mit dem Begriff «Roach Motel» beschrieb.
Sneaking	Informationen, die für die Benutzer_innen von Bedeutung sind, werden verborgen, verschleiert oder verzögert, da die Konsument_innen bei deren Kenntnis die Handlung nicht ausführen würde (Gray et al., 2018, S. 6). Ein Beispiel wäre das Offenlegen von zusätzlichen Kosten erst kurz vor dem Abschluss des Kaufprozesses (Mathur et al., 2019, S. 12).
Interface Interference	Manipulationen im User Interface, welche gewisse Handlungen hervorheben oder priorisieren und damit die Konsument_innen in die Irre führen (Gray et al., 2018, S. 7). So wird bei der Variante «Preselection» beispielsweise die durch das Unternehmen favorisierte Aktion bereits vorselektiert, sodass sich der User aktiv dagegen entscheiden muss (Gray et al., 2018, S. 7) .
Forced Action	Für die Ausführung einer Handlung wird der Konsument gezwungen, eine vom Unternehmen erwünschte weitere Handlung auszuführen (Gray et al., 2018, S. 8). Als Beispiel nennen Bösch et al. (2016, S. 249) die Pflicht der Nutzerregistration mit dem einzigen Zweck, Zugang zu den personenbezogenen Daten der Konsument_innen zu erlangen.
Urgency	Schaffung von Dringlichkeit durch künstliche, zeitliche oder mengenmässige Verknappung, wie beispielsweise beim Einsatz eines Countdown-Timers für die maximal verfügbare Zeit, die den Nutzer_innen für den Kaufprozess zur Verfügung steht (Mathur et al., 2019, S. 86).

2.3.2 Wirkung von Dark Patterns

Erste Studien haben Erkenntnisse dafür geliefert, dass Dark Patterns Nutzer_innen zu Entscheidungen bewegen können, die nicht in ihrem eigenen, besten Interesse liegen (Gunawan et al., 2021, S. 4). Luguri und Strahilevitz (2019, S. 22) prüften beispielsweise im Rahmen eines Experiments anhand eines Lockvogel-Szenarios die Auswirkungen von Dark Patterns und stellen fest, dass beim Einsatz eines aggressiven Dark Patterns sich die Akzeptanzrate zum Lockvogel-Produkt vervierfachte. Gleichzeitig konnten durch die Kombination verschiedener Dark Patterns stärkere Effekte festgestellt werden als in der milden Dark-Pattern-Variante (Luguri & Strahilevitz, 2019, S. 23).
Im Rahmen der Untersuchung der Wirksamkeit von Dark Patterns in Bezug auf die Zustimmung von Nutzer_innen zur Sammlung von personenbezogenen Daten, beobachteten Nouwens et al. (2020, S. 9), dass der Einsatz von Dark Patterns, konkret das Verstecken des Akzeptieren-Buttons, dazu führte, dass der Anteil der User_innen, die dem Tracking zustimmten, um 22 Prozent anstieg

Aufbauend auf der Studie von Moser et al. (2019), welche die Wirkung von Designpraktiken, aber nicht spezifisch Dark Patterns, auf Impulskäufe untersuchte, führten Sin et al. (2022) Forschung spezifisch zu den Effekten von Dark Patterns durch. Im Rahmen von zwei Experimenten wurde aufgezeigt, dass die untersuchten Dark Patterns die Kaufimpulsivität signifikant steigerten, wobei allerdings im Vergleich drei verschiedener Varianten von Dark Patterns keine signifikanten Unterschiede hinsichtlich deren Effektivität festgestellt werden konnten (Sin et al., 2022, S. 23).

Während nun also erste Erkenntnisse zu den Effekten von Dark Patterns vorliegen, weisen Forschende darauf hin, dass es aufgrund der Vielfalt an Dark-Pattern-Typen nicht möglich ist, all deren Effekte zu testen, weshalb sich häufig auf die verbreitetsten Varianten gestützt wird (Sin et al., 2022, S. 3).

Das nachfolgende Kapitel widmet sich der Verbreitung des Phänomens der Dark Patterns insgesamt und gibt ausserdem Erkenntnisse zu der Verbreitung anhand der verschiedenen Typen von Dark Patterns wieder.

2.3.3 Verbreitung von Dark Patterns

Die automatisierte Identifikation von Dark Patterns mittels eines generalisierten Ansatzes, stellt aufgrund des sehr heterogenen Aufbaus von Websites eine Herausforderung dar (Di Geronimo et al., 2020, S. 21; Mathur et al., 2019, S. 13). Aus diesem Grund kamen bei den bisher durchgeführten Studien für die Identifikation häufig eine Kombination aus automatisierten und manuellen Analysen zum Tragen (Mathur et al., 2019, S. 103).

In der Bestrebung, die Verbreitung von Dark Patterns zu quantifizieren, prüften Mathur et al. (2019, S. 27) mittels Semi-Automatisierung über 11'000 beliebte Shoppingwebsites und entdeckten bei über elf Prozent der Sites mindestens ein Dark Pattern. Die Studie von Mathur et al. (2019, S. 27) weist einige Limitationen auf, wie die Beschränkung auf text-basierte Dark Patterns und die Prüfung derer ausschliesslich auf Produktseiten und Checkout-Seiten, womit die Verbreitung wohlmöglich unterschätzt wurde.

Weiter untersuchten Moser et al (2019, S. 1) mittels einer systematischen Inhaltsanalyse 200 beliebte eCommerce-Websites, mit der Absicht, Eigenschaften zu entdecken, welche Impulskäufe fördern. Die Untersuchung umfasst damit auch den Einsatz von Dark Patterns, weist diese allerding nicht dediziert aus (Gunawan et al., 2021, S. 5). Die Untersuchung zeigte, dass 75 Prozent der untersuchten Websites mindestens ein entsprechendes Merkmal aufwiesen (Moser et al., 2019, S. 4).

Im Bereich der mobilen Nutzung analysierten Di Geronimo et al. (2020, S. 1) 240 Mobile Apps in jeweils den ersten zehn Minuten der Nutzung, um darin enthaltene Dark Patterns zu identifizieren und sie in die von Gray et al. (2018) vorgeschlagene Taxonomie einzuordnen. In 95 Prozent der untersuchten Apps wurde mindestens eine Form von Dark Patterns festgestellt und im Durschnitt wurden pro App sieben Formen von Dark Patterns entdeckt (Di Geronimo et al., 2020, S. 1). In der Einordnung der Dark Patterns nach Unterkategorie, die in der Abbildung 2 eingesehen werden kann, wurden die Unterkategorien «False Hierarchy», «Preselection» und «Nagging» als die am weitesten verbreiteten Formen von Dark Patterns identifiziert (Di Geronimo et al., 2020, S. 5).

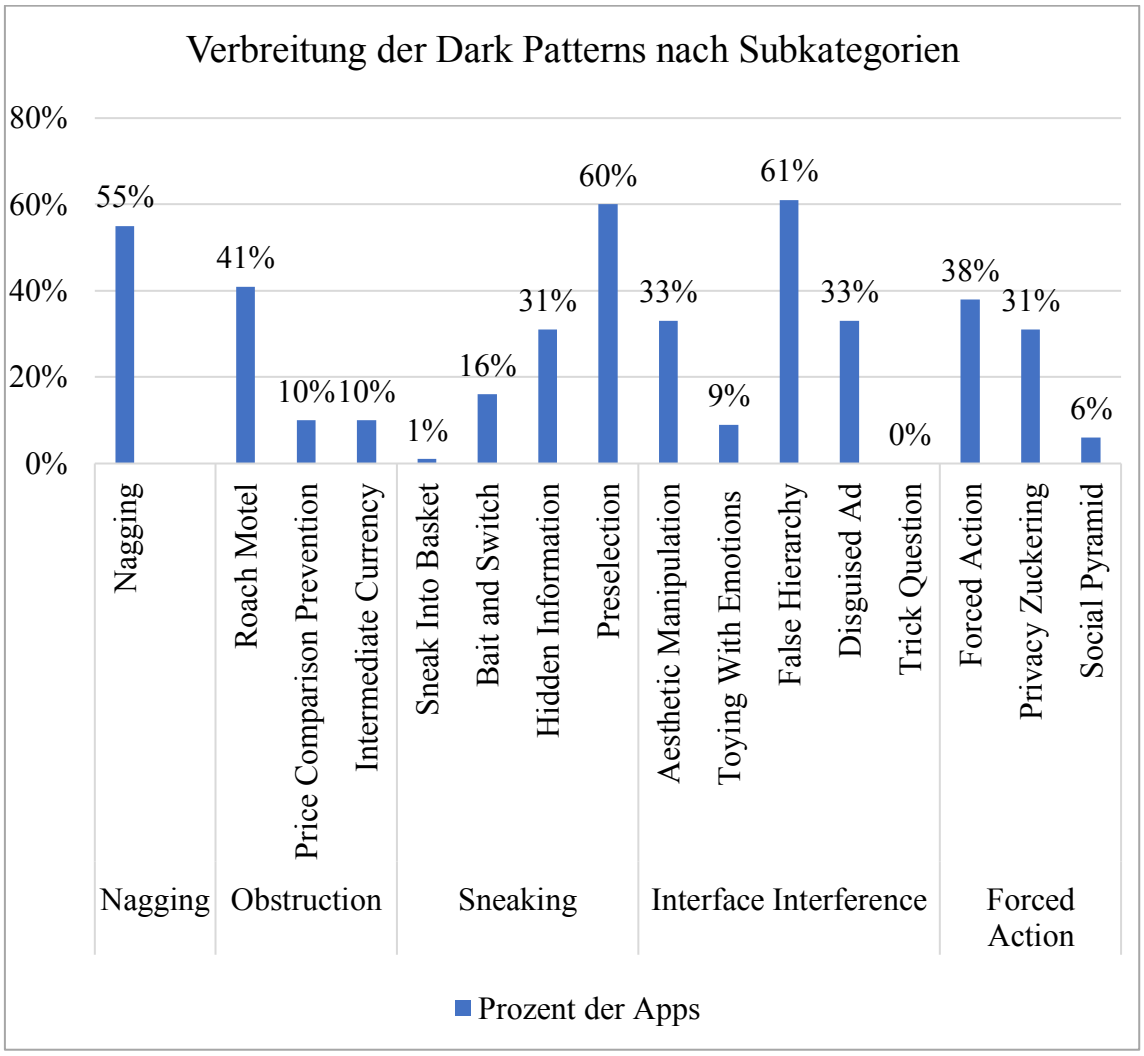


Abbildung 2: Verbreitung der Dark Pattern-Unterkategorien (in Anlehnung an Di Geronimo et al., 2020, S. 6)

Ergänzend zu diesen Erkenntnissen untersuchten Gunawan et al. (2021, S. 2) Unterschiede in den Dark Patterns zwischen Mobile Apps, mobilen Webbrowsern, sowie Desktop Webbrowsern anhand 105 populärer Onlinedienste wie beispielsweise Facebook oder Spotify. Die Resultate zeigten auf, dass der Einsatz von Dark Patterns im Vergleich der genannten Modalitäten hinsichtlich Anzahl, Typ und Eigenschaften inkonsistent ist, was dazu führt, dass Konsument_innen abhängig von der genutzten Modalität Autonomie, Privatsphäre und Kontrolle nicht einheitlich erleben (Gunawan et al., 2021, S. 1). Deckend mit den Erkenntnissen von Di Geronimo et al. (2020), lag der Median der Dark Patterns in der Studie von Gunawan et al. (2021, S. 13) bei sieben bis acht Dark

Patterns pro untersuchtem Dienst. Zusätzlich wurde bei mobilen Geräten mit 85 Prozent die höchste Verbreitung an Dark Patterns festgestellt (Gunawan et al., 2021, S. 2–13).

Zusammenfassend kann festgehalten werden, dass diese ersten Erkenntnisse auf eine weite Verbreitung von Dark Patterns hindeuten, wobei starke Limitationen hinsichtlich der genutzten Methoden zur Identifikation zu nennen sind, was die Aussagekraft beeinträchtigt.

Relativ gut untersucht ist die Verbreitung von Dark Patterns in Datenschutzhinweisen, im spezifischen in Cookie-Zustimmungshinweisen (Gunawan et al., 2021, S. 4). Als Cookie-Zustimmungshinweis (auch Cookie-Hinweis oder Cookie-Banner genannt) werden Banner verstanden, welche Website-User_innen über den Einsatz von Cookies durch die Website und allfällige Drittparteien informieren und entweder deren explizite oder implizite Zustimmung erfragen (Degeling et al., 2019, S. 3). Die Verbreitung von Dark Patterns in Cookie-Zustimmungshinweisen wird im nachfolgenden Kapitel gesondert erörtert, nachdem einleitend aufgezeigt wird, welche Rechtsgrundlagen zur Einführung von Cookie-Zustimmungshinweisen führten.

2.3.4 Verbreitung von Dark Patterns in Cookie-Zustimmungshinweisen

Cookies sind kleine Informationseinheiten, die von Websites in Browsern platziert und gespeichert werden, während die Nutzer_innen im Internet surfen (Mellet & Beauvisage, 2020, S. 111). Die durch die Cookies abgespeicherten Daten über die Nutzer_innen, ermöglichen die Personalisierung von Onlinewerbung basierend auf den Eigenschaften und Interessen der Nutzer_innen (Sanchez-Rola et al., 2019, S. 340).

Cookie-Zustimmungshinweise wurden weitgehend als Reaktion auf neue Datenschutz-richtlinien, wie die ePrivacy-Richtlinie der Datenschutzgrundverordnung der Europäischen Union (DSGVO), welche im Mai 2018 in Kraft trat, ausgerollt (Utz et al., 2019, S. 974). Die neue ePrivacy-Richtline sah eine Verschärfung vor, in dem mit Inkrafttreten die explizite Zustimmung der Nutzer_innen zu Cookie-Tracking, mit Ausnahme der für den Betrieb der Website notwendigen Cookies, verlangt wurde (Sanchez-Rola et al., 2019, S. 374). Weiter wird im entsprechenden Artikel zur expliziten

Zustimmung ausgeführt, dass diese aus freiem Willen, eindeutig, informiert und jederzeit widerrufbar erfolgen muss (Utz et al., 2019, S. 974).

Die europäische Datenschutzgrundverordnung erreichte auch ausserhalb der EU Relevanz, da sie Anwendung findet, sobald personenbezogene Daten von in der EU ansässigen Personen verarbeitet werden, oder Waren und Dienstleistungen an Personen in der EU angeboten werden (Sanchez-Rola et al., 2019, S. 341). Weiter folgte nebst der europäischen Datenschutzgrundverordnung auch eine entsprechende Richtlinie für den kalifornischen Staat, der California Consumer Privacy Act (CCPA), welcher im Januar 2020 in Kraft trat (Soe et al., 2020, S. 1; Utz et al., 2019, S. 973).

Für den Umgang mit in der Schweiz ansässigen Personen genügt gemäss aktuell geltendem Recht noch ein entsprechender Hinweis in der Datenschutzerklärung und die Möglichkeit eines «Opt-Outs» (Schweizerische Eidgenossenschaft, 1997). Der Cookie-Hinweis nach Schweizer Recht hat damit aktuell rein informativen Charakter und es wird noch keine explizite Zustimmung für das Tracking benötigt (Perrot, 2019).

Allerdings wurde auch in der Schweiz eine Revision des Datenschutzgesetz veranlasst, welches der DSGVO angeglichen wird (Sury, 2017, S. 222). Die Gesetzesrevision soll gemäss aktuellem Stand per 2023 in Kraft treten und beabsichtigt bei der Erhebung und Bearbeitung personenbezogener Daten mehr Transparenz zu schaffen und die Selbstbestimmung der betroffenen Personen über ihre Daten zu stärken (Schweizerische Eidgenossenschaft, 2022).

Mit Inkrafttreten der DSGVO im Mai 2018 wurde ein Anstieg der Verbreitung von Cookie-Zustimmungshinweise von 46.1 Prozent im Januar 2018 auf 62.1 Prozent im Mai des selben Jahres festgestellt (Degeling et al., 2019, S. 2). Mit deren Verbreitung wurden ausserdem Consent-Management-Anbieter (englisch: Consent Management Providers, CMPs) als Akteure eingeführt, welche für die Einholung der Zustimmung und die Weitergabe dieser an die Werbetreibenden beauftragt sind (Matte et al., 2020, S. 791). Im Interesse die Nutzer_innen zu einer Einwilligung der Datenerhebung und -weitergabe zu verleiten, finden auf vielen Websites Nudging oder auch Dark Patterns Anwendung

(Gunawan et al., 2021, S. 4; Utz et al., 2019, S. 974). Die Erkenntnisse der Forschung zu letzterem wird nachfolgend erläutert.

Utz et al. (2019, S. 974) untersuchten ein Sample von 1'000 Cookie-Zustimmungserklärungen auf Gemeinsamkeiten in deren Gestaltungsmerkmalen, wie beispielsweise die Positionierung auf der Webseite oder die möglichen Antwortoptionen. Dabei wurde festgestellt, dass bei 57.4 Prozent eine Manipulationspraxis wie Nudging oder Dark Patterns zum Einsatz kommt, wobei die beiden Praktiken nicht gesondert ausgewiesen wurden (Utz et al., 2019, S. 976). Weiter konnten die Forschenden in einem Experiment starke Effekte von Nudges, wie die Hervorhebung des Akzeptieren-Buttons, und Vorauswahlen (Preselection) auf die Zustimmung zum Hinweis aufzeigen (Utz et al., 2019, S. 981).

In einer weiteren quantitativen Studie untersuchten Nouwens et al. (2020, S. 1) die Designs der fünf gängigsten Consent-Management-Anbieter auf den führenden 10’000 Websites des Vereinigten Königreichs. Sie stellten fest, dass bei 32.5 Prozent der untersuchten Websites, weiterhin nur die implizite Zustimmung erfragt wird und dass der Grossteil der Consent-Management-Anbieter die Ablehnung des Trackings wesentlich schwieriger gestalten als die Annahme (Nouwens et al., 2020, S. 5). So konnte beispielsweise bei nur 12.6 Prozent der Websites die Alle-ablehnen-Option mit gleich vielen oder weniger Klicks erreicht werden wie die Alle-akzeptieren»-Option, was in die Dark-Pattern-Kategorie «Obstruction» eingeordnet werden könnte (Nouwens et al., 2020, S. 5). Die Abbildung 3 zeigt ein Beispiel für den genannten Anwendungsfall des Obstruction-Dark-Patterns auf dem Onlineshop Zalando. Die Ablehnung der Cookies kann nur durch einen zusätzlichen Klick und anschliessende Abwahl einzelner Einstellungen erreicht werden.

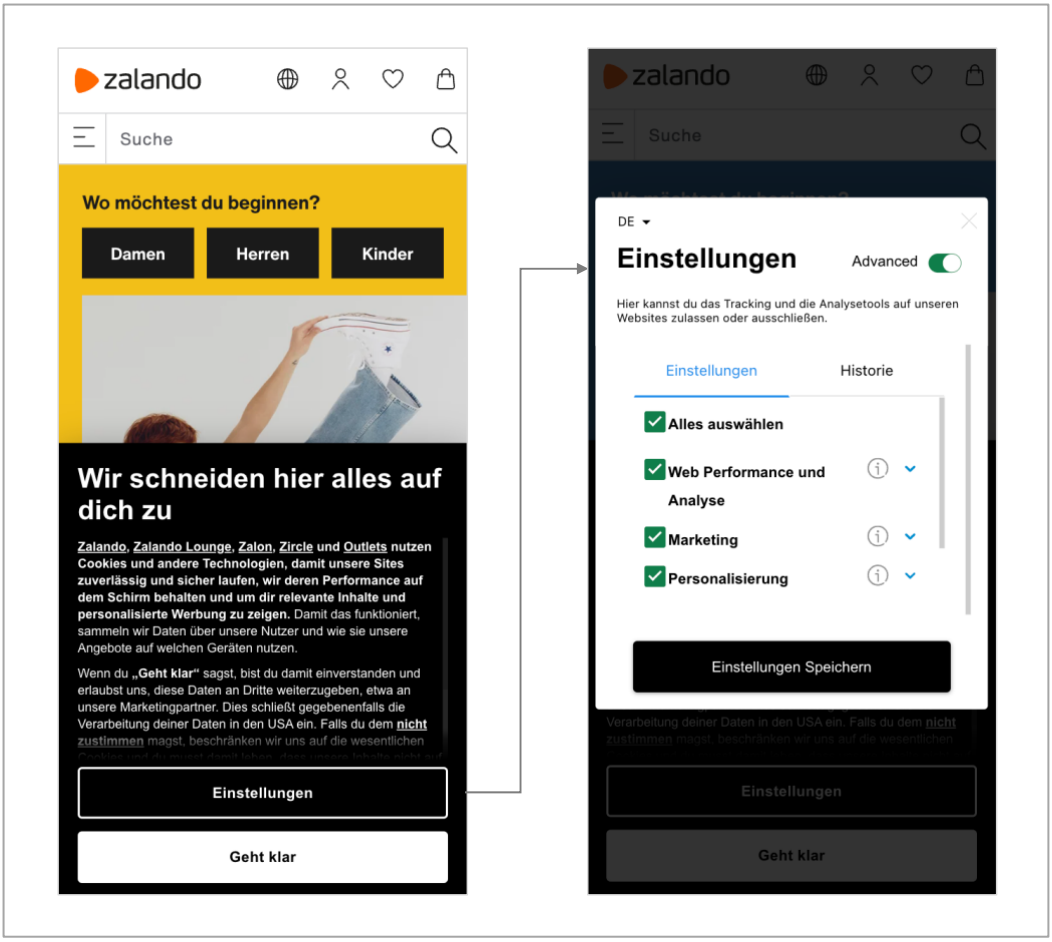


Abbildung 3: Beispiel Dark Pattern auf Cookie-Zustimmungshinweis (Zalando, o. J.)

Weiter sind Vorauswahlen der datenschutzfeindlichen Antwortmöglichkeit, was gemäss der Kategorisierung von Gray et al. (2018, S. 6) als Dark Pattern der Kategorie «Sneaking» klassifiziert wurde, in Cookie-Zustimmungshinweisen weit verbreitet (Matte et al., 2020, S. 792). So stellten Matte et al. (2020, S. 792) in der Analyse von 560 Websites fest, dass bei 46.5 Prozent die datenschutzfeindlichen Antwortmöglichkeiten vorselektiert wurden.

Analog der im Kapitel 2.3.3 vorgestellten Studie von Di Geronimo et al. (2020) prüften Soe et al. (2020, S. 4) ebenfalls die Verbreitung von Dark Patterns anhand der Taxonomie von Gray et al. (2018), in diesem Fall wurden Cookie-Zustimmungshinweise eines Samples von 300 Websites untersucht. Bei 297 von 300 Websites wurden Dark Patterns für die Einholung der Zustimmung zu den Cookies eingesetzt (Soe et al., 2020, S. 10). Die meistverbreiteten Kategorien waren dabei «Obstruction», bei 43 Prozent der

Hinweise identifiziert, sowie «Interface Interference» bei 45.3 Prozent der Hinweise (Soe et al., 2020, S. 5).

«Obstruction» erfolgt bei Cookie-Zustimmungshinweisen meist, indem die Alle ablehnen-Option hinter einer getrennten Seite versteckt wird, welche nur mittels Klick auf einen Button mit missverständlichem Text wie «Mehr erfahren» erreicht werden kann (Soe et al., 2020, S. 5). Zu «Interface Interference» werden versteckte Informationen, Vorauswahl oder ästhetische Manipulation gezählt, wie beispielsweise das Verstecken der Ablehnen-Option durch verschleierndes Design (Soe et al., 2020, S. 5).

In Bezug auf die manuelle Sammlung und Auswertung der Hinweise weisen Soe et al. (2020, S. 5) auf eine starke Diskrepanz in der Klassifikation der Dark Patterns und damit eine tiefe Interrater-Reliabilität mit 67 Prozent hin. Dies kann wiederum mitunter auf die unzureichende Beschreibung von Dark Patterns zurückgeführt werden, was ihre Charakterisierung erschwert (Soe et al., 2020, S. 5).

2.3.5 Regulation von Dark Patterns

Nachdem in den vorhergehenden Kapiteln die Verbreitung und Wirkung der Dark Patterns erläutert wurde, soll an dieser Stelle ein Überblick über die regulatorischen Massnahmen in Bezug auf Dark Patterns geboten werden. Die Aufführung hat dabei keinen Anspruch auf Vollständigkeit, sondern nennt die hinsichtlich der Tragweite relevantesten regulatorischen Massnahmen.

Mit steigender Verbreitung von Dark Patterns werden auch regulatorische Massnahmen zu deren Einschränkung zunehmend thematisiert (Lukoff et al., 2021, S. 2). Während in der Gesetzgebung der Europäischen Union Dark Patterns nicht spezifisch erwähnt werden, wurden spezifische Praktiken wie beispielsweise die Vorauswahl der Zustimmung in Cookie-Hinweisen verboten (Hermstrüwer, 2017, S. 23). Ähnliches wurde im Staat Kalifornien im Jahre 2021 durch eine Anpassung des California Consumer Privacy Act erreicht, in dem der Einsatz von Dark Patterns in Zusammenhang mit dem Datenschutz verboten wurde (Sin et al., 2022, S. 22).

Auf nationaler Ebene wurde in den Vereinigten Staaten im Rahmen des DETOUR Acts (Deceptive Experiences to Online Users Reduction Act) ein Standard vorgeschlagen, welcher den Einsatz von Dark Patterns explizit erwähnt und als rechtwidrig erklärt (Mathur et al., 2021, S. 18). Die Durchsetzung dieser Gesetzgebungen könnte sich allerdings aufgrund der Vielfalt der Strategien und des Mangels an Konzeptionalisierung als schwierig erweisen (Mathur et al., 2021, S. 25; Sin et al., 2022, S. 23).

Ergänzend zur Regulation durch die Gesetzgebung schlugen verschiedene Forschende vor, Dark Patterns mittels Aufklärung und Sensibilisierung zu bekämpfen und schufen deshalb Plattformen für den Austausch zur Thematik (Brignull, 2010b; Maier & Harr, 2020, S. 180; Mathur et al., 2021, S. 25).

2.3.6 Dark Pattern Verbrauchergefährdung

«Consumer vulnerability» oder zu Deutsch «Verbrauchergefährdung» beschreibt «ein[en] Zustand der Machtlosigkeit, die durch ein Ungleichgewicht in den Marktinteraktionen oder durch den Konsum von Marketingbotschaften und Produkten entsteht» (Baker et al., 2005, S. 134). Ursprung für die Gefährdung sind dabei der eingeschränkte Zugang oder die eingeschränkte Kontrolle über Ressourcen der Konsument_innen (Hill & Sharma, 2020, S. 554). Die genannten Ressourcen können dabei individueller, interpersoneller oder struktureller Natur sein (Hill & Sharma, 2020, S. 559). In der Tabelle 2 wird die Kategorisierung der Ressourcen genauer beschrieben und mit Beispielen ausgeführt.

Tabelle 2: Individuelle, interpersonelle und strukturelle Ressourcen (in Anlehnung an Hill & Sharma, 2020, S. 559)

Kategorie	Beschrieb	Beispiele
Individuelle Ressourcen	Psychologische Merkmale, Physiologische Merkmale, Fähigkeiten oder Besitztümer	Kognitive Ressourcen, Mobilität, Kompetenzen, Finanzen etc.

Interpersonelle Ressourcen	Soziales Kapital, Gefühl der Zugehörigkeit, Unterstützung durch das Umfeld	Status, Netzwerk an Freunden, Familie und Kollegen
Strukturelle Ressourcen	Kontextuelle Ressourcen, Umwelt	Verfügbarkeit von Gütern und Dienstleitungen, Verfügbarkeit von Nahrung, Wasser und Raum

Weiter wird zwischen globaler, holistischer Vulnerabilität und situationsspezifischer Vulnerabilität, welche abhängig vom zeitlichen und räumlichen Kontext ist, unterschieden (Hill & Sharma, 2020, S. 562).

Nudges nutzten psychologische Schwachstellen von Nutzer_innen aus, um deren Entscheidungen zu beeinflussen (Thaler & Sunstein, 2009). Bei Dark Patterns im spezifischen bringt die Ausnutzung dieser Schwachstellen negative Konsequenzen mit sich (Konsumentverket, 2021, S. 16). Gemäss der Theorie der digitalen Marktmanipulation sind alle Konsument_innen unter gewissen Umständen, wie beispielsweise in Stresssituationen, vulnerabel für manipulative Techniken der Verhaltensarchitektur (Calo, 2014, S. 1033). Neben diesen situationalen Faktoren der Vulnerabilität wies aber beispielsweise Sunstein (2020, S. 9) darauf hin, dass die Konsequenzen von Sludges für vulnerable Individuen wie ältere Personen, besonders stark ausfallen können. Im Bereich der Dark Patterns liegt erst wenig Forschung zur Frage vor, ob nutzergruppenspezifische Unterschiede hinsichtlich der Dark-Pattern-Effektivität und damit der Konsumentengefährdung bestehen. Im Folgenden werden erste Erkenntnisse zu globalen Vulnerabilitätfaktoren im Bezug auf Dark Patterns vorgestellt.

Di Geronimo et al. führten den Begriff «Dark Pattern Blindheit» ein, um Personen zu beschreiben, die nicht in der Lage sind, Dark Patterns zu erkennen (Di Geronimo et al., 2020). Mittels qualitativer Befragung identifizierten Di Geronimo et al. (2020), dass

Nutzer bei vorheriger Information, dass Dark Patterns auftreten könnten, diese eher erkannten, was vermuten lässt, dass Aufklärungsmassnahmen die Effekte von Dark Patterns mindern könnten (Di Geronimo et al., 2020, S. 9).

Ersten Studien zufolge wird der Bildungsstand als möglicher Faktor der Vulnerabilität vermutet. So stellten Luguri und Strahilevitz (2019, S. 28) in einer experimentellen Studie fest, dass Proband_innen mit tieferem Bildungsstand signifikant stärker auf «milde» Dark Patterns reagierten, als Proband_innen mit höherer Bildung. Bei «aggressiven» Dark Patterns konnte dies allerdings nicht festgestellt werden (Luguri & Strahilevitz, 2019, S. 28).

Zu ähnlichen Erkenntnissen gelangten auch Bongard-Blanchy et al. (2021, S. 774) in deren Studie Personen mit niedrigerem Schulabschluss weniger in der Lage waren, Dark Patterns zu erkennen als solche mit höherem Schulabschluss.

Gleichzeitig zeigten Proband_innen mit höherer Bildung ein stärkeres Bewusstsein für den Einfluss von Design auf deren Entscheidungen und Verhalten, sowie für die potenziellen Schäden, die dadurch entstehen können (Bongard-Blanchy et al., 2021, S. 769). Deshalb kann vermutet werden, dass Personen mit tieferem Bildungsstand, aufgrund des geringeren Bewusstseins über mögliche manipulative Designpraktiken, vulnerabel für solche sind. Ergänzend zu den Erkenntnissen bezüglich des Bildungsstandes stellten Bongard-Blanchy et al. (2021, S. 774) fest, dass Personen über 40 Jahre weniger gut im Stande waren, Dark Patterns zu erkennen.

In einer Befragung zum Thema «Abonnement-Fallen» im Internet wurde weiter festgestellt, dass Personen zwischen 50 und 64 Jahren am anfälligsten für diese sind (Citizens Advice, 2016, S. 2). Hierbei wurde nicht konkret der Einsatz von Dark Patterns geprüft, allerdings werden bei Abonnement-Fallen im Internet häufig Dark Patterns der Kategorie «Sneaking» entsprechen der Taxonomie von Gray et al. (2018, S. 6) eingesetzt.

Da Dark Patterns im Internet Anwendung finden, ist hier auch zu berücksichtigen, dass ältere Personen aufgrund in der Regel geringerer digitaler Kompetenzen oder digitaler

Ausgrenzung anfälliger für Gefahren im Internet, wie Dark Patterns, sind (Competition & Markets Authority, 2019, S. 12).

Im nachfolgenden Kapitel wird deshalb die Thematik der digitalen Kompetenz, auch Digital Literacy genannt, genauer beleuchtet.

2.4 Digitale Kompetenz

Heutzutage besteht eine Vielzahl an Definitionen für Digitale Kompetenz und aufgrund der rasanten und kontinuierlichen technologischen, kulturellen und sozialen Entwicklungen wird deren Nutzung und Bedeutung ständig neu definiert (Helsper, 2008, S. 56).

Für die vorliegende Arbeit wird auf die Definition der European Information Society gestützt, welche Digitale Kompetenz wie folgt definiert: «Digitale Kompetenz beschreibt das Bewusstsein, die Einstellung und die Fähigkeit des Einzelnen, digitale Werkzeuge und Infrastruktur angemessen zu nutzen, um digitale Ressourcen zu identifizieren, auf sie zuzugreifen, sie zu verwalten, zu integrieren, zu bewerten, zu analysieren und zu synthetisieren, neues Wissen aufzubauen, mediale Ausdrucksformen zu schaffen und mit anderen zu kommunizieren, im Kontext bestimmter Lebenssituationen, um konstruktives soziales Handeln zu ermöglichen, und diesen Prozess zu reflektieren»(Martin, 2005, S. 135-136).

Aus der Definition wird bereits klar, dass Digitale Kompetenz sehr umfassend ist und eine Vielfalt an Fähigkeiten beinhaltet, die im Umgang mit Informations- und Kommunikationstechnologie und im Internet benötigt werden (Office for Official Publications of the European Communities, 2003, S. 3). Digitale Kompetenz teil starke konzeptionelle Gemeinsamkeiten mit weiteren Kompetenzen wie der Medienkompetenz, Nachrichtenmedienkompetenz oder der Informationskompetenz, sodass einige Forschende sogar davon sprechen, dass Digitale Kompetenz sich aus anderen Kompetenzen zusammensetzt (Koltay, 2011, S. 216; Rodríguez-de-Dios et al., 2018, S. 187).

2.4.1 Fertigkeitsdimensionen der Digitalen Kompetenz

Mit dem Ziel, Digitale Kompetenz zu charakterisieren, brachen Forschende diese in verschiedene Dimensionen auf (Rodríguez-de-Dios & Igartua, 2016, S. 58). Eshet-Alkalai (2004, S. 94) beispielsweise definierte die fünf Dimensionen: foto-visuelle Kompetenz, Reproduktionskompetenz, Informationskompetenz, Verzweigungs-kompetenz und sozio-emotionale Kompetenz.
Aufbauend auf dem konzeptionellen Rahmen von Eshet-Alkalai entwickelten Rodríguez-de-Dios & Igartua (2016, S. 60) fünf Fertigkeits-Dimensionen, die das breite Spektrum des digitalen Raums, nebst dem Internet, besser repräsentieren sollten und ebenso Fähigkeiten berücksichtigen, die für die Risikoeinschätzung und das Erkennen von Gefahren benötigt werden. In der vorliegenden Masterarbeit wird auf ebendiese Dimensionen zurückgegriffen, da Dark Patterns als eine Gefahr im Umgang mit digitalen Technologien betrachtet werden können, weshalb die Risikoeinschätzung in diesem Kontext sehr relevant ist (Luguri & Strahilevitz, 2019, S. 35).

Die fünf Dimensionen werden in der folgenden Tabelle 3 vorgestellt und genauer beschrieben.

Tabelle 3: Fertigkeitsdimensionen der digitalen Kompetenz (in Anlehnung an Rodríguez-de-Dios & Igartua, 2016, S. 60)

Fertigkeit	Beschrieb
Technologische oder instrumentelle Fertigkeit	Die Fertigkeit, digitale Technologien effektiv einzusetzen, wie beispielsweise die Auswahl einer geeigneten Software für eine bestimmte Aufgabenstellung (Rodríguez-de-Dios & Igartua, 2016, S. 60).
Kommunikationsfertigkeit	Die Fertigkeit, kommunikative Botschaften, wie beispielsweise eine E-Mailnachricht, auf den Kontext und die Empfänger_innen anzupassen und korrekt zu interpretieren (Rodríguez-de-Dios & Igartua, 2016, S. 60).

Informationsfertigkeit	Die Fertigkeit, gewünschte Informationen im digitalen Raum zu finden, analysieren, synthetisieren, vergleichen, bewerten und verstehen (Rodríguez-de-Dios & Igartua, 2016, S. 60).
Kritische Analyse-Fertigkeit	Die Fertigkeit, empfangene Informationen kritisch zu analysieren und allfällige Gefahren zu erkennen (Rodríguez-de-Dios & Igartua, 2016, S. 60).
Sicherheitskompetenz	Die Fertigkeit im Umgang mit persönlichen Informationen und Schutz derselben im digitalen Raum (Rodríguez-de-Dios & Igartua, 2016, S. 60).

2.4.2 Bedeutung Digitaler Kompetenz und die digitale Kluft

Aufgrund des enormen Wachstums digitaler Technologien wirkt sich die Beherrschung von Informations- und Kommunikationstechnologien mittlerweile auf jeden Aspekt des Lebens und täglicher Beziehungen aus (Jacobs et al., 2014, S. 626). Aus diesem Grund wird in der Literatur darauf hingewiesen, dass es notwendig ist, dass alle Individuen, unabhängig derer Erfahrungen und Herkunft, über die notwendigen Fähigkeiten und Kompetenzen verfügen, um Aufgaben und Probleme in digitalen Umgebungen zu lösen und damit persönlichen, sozialen und wirtschaftlichen Erfolg im 21.Jahrhundert erreichen zu können (Martin & Grudziecki, 2006, S. 256; Reddy et al., 2020, S. 66).

Personen mit unzureichender Digitaler Kompetenz machen diese ausserdem anfällig für Betrug, Schädigung und Manipulation (Kucuk, 2016, S. 526). Die Förderung Digitaler Kompetenz ist essenziell, um einer Ausgrenzung und Marginalisierung von vulnerablen Personen entgegenzuwirken (Jacobs et al., 2014, S. 626). In diesem Zusammenhang wird von «digital divide» oder zu Deutsch von einem digitalen Graben gesprochen, der sich zwischen Nutzergruppen, abhängig von deren Nutzung des Internets, ergibt (DiMaggio & Hargittai, 2001, S. 2).

Das Konzept des digitalen Grabens entstand in den 1990er Jahren (Lythreatis et al., 2022, S. 2) und beschrieb damals die reine binäre Trennung nach Personen mit Zugang zum

Internet und solchen ohne Zugang (Riggins & Dewan, 2005, S. 298). Seither wurde das Konzept des digitalen Grabens erweitert und die eben genannte Trennung wird als erstes Level des digitalen Grabens bezeichnet (Lythreatis et al., 2022, S. 2). Das zweite Level des digitalen Grabens fokussiert sich auf Unterschiede hinsichtlich der digitalen Kompetenzen und der digitalen Nutzung (Riggins & Dewan, 2005; van Dijk, 2005). Das dritte Level wird auch digitale Ergebniskluft genannt und beschreibt die Ungleichheit der Ergebnisse wie beispielsweise die Produktivität, die durch den Einsatz digitaler Medien entsteht (Wei et al., 2011, S. 171).

Als Determinanten für den digitalen Graben wurden vorwiegend soziodemografische und sozioökonomische Faktoren wie Einkommen, Alter, Bildungsgrad, Ethnizität etc. identifiziert (Hidalgo et al., 2020).

2.4.3 Digitale Kompetenz in der Schweiz

In einer Erhebung des Bundesamt für Statistik (2021, S. 3) zur zweiten Stufe des digitalen Grabens und damit zur digitalen Kompetenz ergab, dass 46 Prozent der Bevölkerung über erweiterte allgemeine digitale Kompetenzen verfügen, während 28 Prozent über grundlegende Kompetenzen und 20 Prozent über geringe oder gar keine digitale Kompetenzen verfügen.

Als Faktoren für Unterschiede hinsichtlich Digitaler Kompetenzen in der Schweiz konnten der Bildungsstand, die sozioprofessionelle Kategorie, der Migrationsstatus, das Alter, sowie die selbstwahrgenommene finanzielle Situation des Haushalts identifiziert werden (Bundesamt für Statistik, 2022a, S. 6). Personen mit lediglich obligatorischem Schulabschluss haben der Studie zufolge das höchste Risiko für geringe digitale Kompetenzen (Bundesamt für Statistik BFS, 2021, S. 8). Im Bereich sozioprofessioneller Kategorien ist das Risiko für ungelernte Arbeitskräfte am höchsten (Bundesamt für Statistik, 2021, S. 8). Weiter haben in der Schweiz geborene Ausländerinnen und Ausländer die höchste Wahrscheinlichkeit, lediglich über geringe digitale Kompetenzen zu verfügen (Bundesamt für Statistik, 2021, S. 8). Weniger starke Effekte wurden im Bereich des Alters und der finanziellen Situation gemessen, wobei ältere Personen und

Personen mit einer «schwierigen» finanziellen Situation das höchste Risiko für eine geringe Digitale Kompetenz aufwiesen (Bundesamt für Statistik, 2021, S. 8).

Während die oben genannten Resultate auf Daten von einer Erhebung vor der Covid-19-Pandemie basieren, liegen erste Ergebnisse einer Erhebung aus dem Jahr 2021 vor. Dabei wurden starke altersspezifische Unterschiede im Bereich der erweiterten Digitalen Kompetenz festgestellt (Bundesamt für Statistik, 2022a). Die Verteilung der erweiterten Digitalen Kompetenz nach Altersgruppe kann in der Abbildung 4 eingesehen werden. Die Grafik verdeutlicht, dass die erweiterten Digitalen Kompetenzen mit zunehmendem Alter stark abnehmen (Bundesamt für Statistik, 2022a).

Weitere Resultate der Studie sind noch ausstehend, wobei davon auszugehen ist, dass sich durch die Covid-19-Pandemie einige Entwicklungen im Bereich der Digitalen Kompetenz ergeben haben (Bundesamt für Statistik BFS, 2021, S. 8).

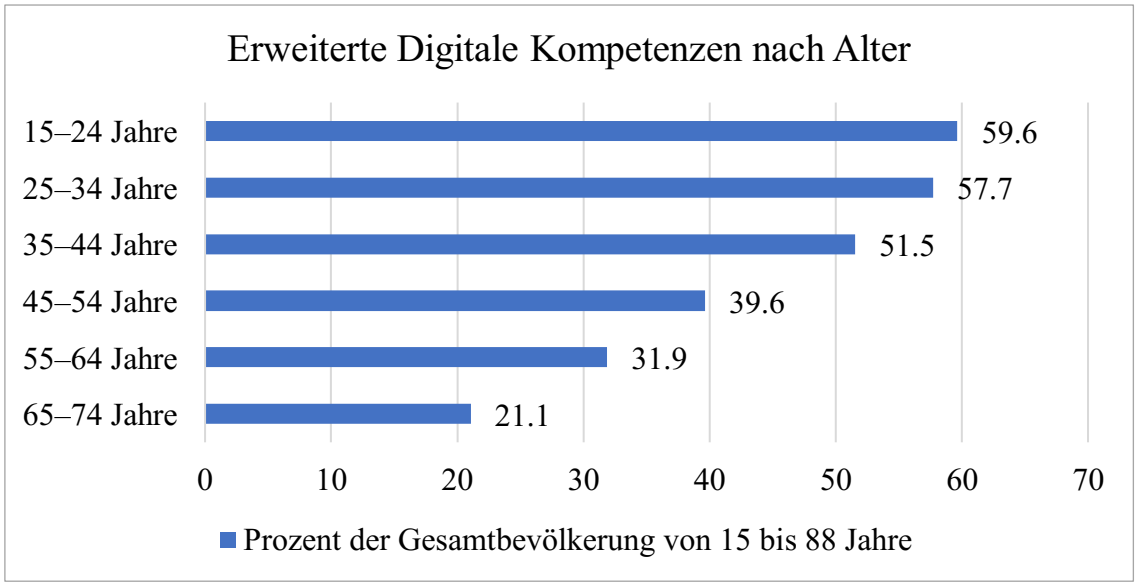


Abbildung 4: Erweiterte Digitale Kompetenzen nach Alter in der Schweiz (in Anlehnung an Bundesamt für Statistik, 2022a)

2.4.4 Messung von Digitaler Kompetenz

Die Messung von Digitaler Kompetenz beschäftigt die Forschung seit Jahren (Tondeur et al., 2017, S. 3). Dabei ist vor allem mangelnde Aktualität aufgrund rascher und

tiefgreifender technologischer Veränderungen eine Herausforderung für die Entwicklung von Messmethoden (Wilson et al., 2015, S. 79).

Digitale Kompetenz wird mittels verschiedener Methoden wie Befragung, Computer-basierter Fähigkeitstest oder auch Wissenstests erhoben, wobei Selbsteinschätzungs-Fragebogen die häufigste Form der Messung darstellen (Kuhlemeier & Hemker, 2007, S. 462). Verschiedene Forschende empfehlen die Messung via Fähigkeitstests, da bei der Selbsteinschätzung die Fertigkeiten häufig unter- oder überschätzt werden und Fähigkeitstests somit aussagekräftiger sind (Sonck & de Haan, 2013, S. 82). Allerdings sind diese sehr kosten- und zeitintensiv in der Umsetzung, weshalb häufig auf Selbsteinschätzungs-Fragebogen zurückgegriffen wird (van Deursen et al., 2012, S. 827). Diese Methode ist kostengünstig umzusetzen und hat den weiteren Vorteil, dass in kurzer Zeit eine breite Anzahl an Fertigkeiten abgefragt werden können (Kuhlemeier & Hemker, 2007, S. 462).

2.5 Entwicklung der Hypothesen und des konzeptionellen Modells

Im folgenden Kapitel werden die wichtigsten Erkenntnisse aus dem Stand des Wissens zusammengefasst und darauf aufbauend Hypothesen für die vorliegende Forschung formuliert. Ergänzend dazu wird das konzeptionelle Modell des Forschungsdesigns vorgestellt.

2.5.1 Herleitung der Hypothesen

Der Einsatz von Dark Patterns soll am Anwendungsfall von Cookie-Hinweisen untersucht werden, da Cookie-Hinweise heutzutage auf fast allen Websites Anwendung finden und dabei bei einem Grossteil der Hinweise Dark Patterns eingesetzt werden (Graßl et al., 2021, S. 2). Weiter finden sich in Cookie-Hinweisen häufig die Dark-Pattern-Typen False Hierarchy, Preselection und Nagging wieder (Graßl et al., 2021, S. 4), welche gleichzeitig gemäss Geronimo et al. (2020, S. 6) die drei am weitverbreitetsten Dark-Pattern-Typen darstellen.

Gemäss der Privacy Calculus Theory wäre zu erwarten, dass die Proband_innen das Sammeln der Cookies ablehnen (Smith et al., 2011, S. 1001). Wird die Sammlung von

Cookies trotzdem akzeptiert, weist dies darauf hin, dass, durch das Dark-Pattern verursacht, auf System-1-Denken zurückgegriffen und das Prinzip der Rationalität verletzt wird (Smith et al., 2011, S. 1000).

Wie in Kapitel 2.3.6 eingeführt wurde, stellten Di Geronimo et al. (2020, S. 9) fest, dass Nutzer_innen bei vorheriger Information, dass Dark Patterns auftreten könnten, diese eher erkannten. Darauf aufbauend soll untersucht werden, ob bei Nutzer_innen, welche Dark Patterns erkennen, diese auch weniger wirksam sind.

Daraus werden die folgenden Hypothesen abgeleitet:

H1: Der Einsatz von Dark Patterns wirkt sich positiv auf die Zustimmung zu den Cookies aus.

H2: Die Erkennung des Dark Patterns mindert die Wirkung von Dark Patterns auf die Zustimmung zu den Cookies.

In Kapitel 2.3.6 wurden Studien vorgestellt, bei denen unterschiedliche Effekte abhängig vom Alter und dem Bildungsstand festgestellt wurden. Kombiniert mit den Erkenntnissen zu soziodemografischen Faktoren, welche die Ausprägung Digitaler Kompetenz erklären, wird vermutet, dass die Digitale Kompetenz die Wirkung von Dark Patterns moderiert. Daraus lassen sich die folgenden Hypothesen ableiten:

H3a: Digitale Kompetenz wirkt sich positiv auf die Fähigkeit Dark Patterns zu erkennen aus.

H3b: Digitale Kompetenz mindert die Auswirkung von Dark Patterns auf die Zustimmung zu den Cookies.

H3c: Digitale Kompetenz wirkt sich negativ auf die die Zustimmung zu den Cookies aus.

2.5.2 Konzeptionelles Modell

Die im vorhergehenden Kapitel entwickelten Hypothesen werden im konzeptionellen Modell in der Abbildung 5 dargestellt und die Variablen in der Tabelle 4 verordnet.

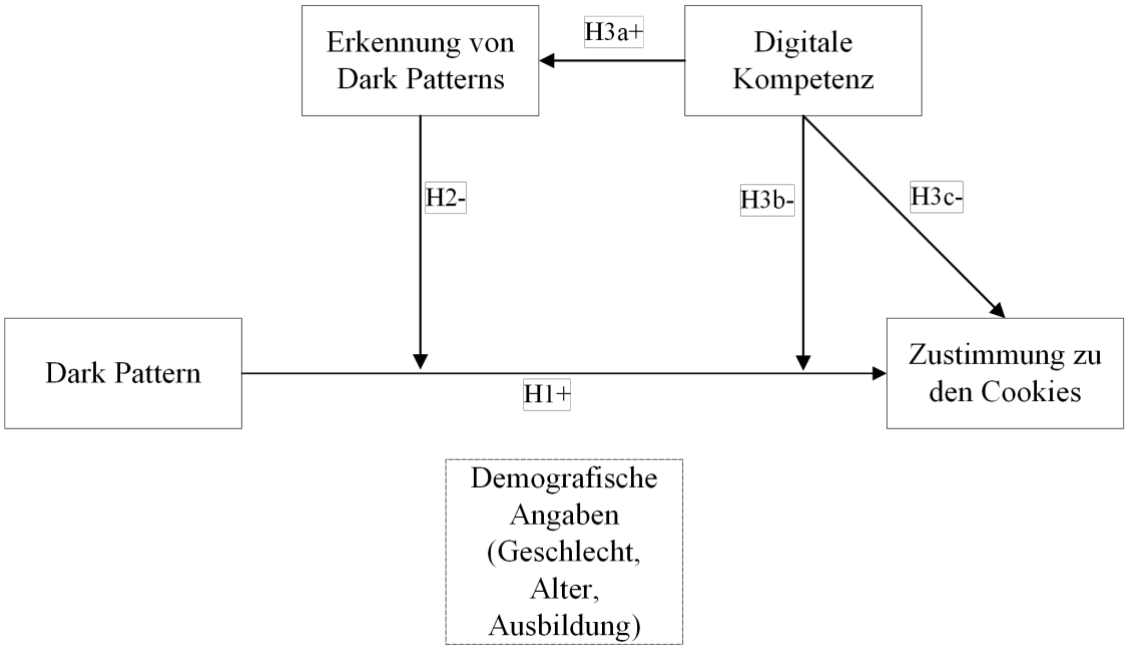


Abbildung 5: Konzeptionelles Modell des Forschungsdesigns

Tabelle 4: Variablen des Experiments

Konstrukt	Einfluss
Einsatz Dark Pattern	Unabhängige Variable (x)
Digitale Kompetenz	- Potenzielle Moderation der Auswirkung von Dark Patterns auf die Zustimmung zu den Cookies (negativ) - Potenzielle positive Wirkung auf die Erkennung von Dark Patterns - Potenzielle negative Wirkung auf die Zustimmung zu den Cookies

Fähigkeit Dark Patterns zu Erkennen	Potenzielle Moderation der Auswirkung von Dark Patterns auf die Zustimmung zu den Cookies (negativ)
Zustimmung zu Cookies	Abhängige Variable (y)
Demografische Angaben (Alter, Geschlecht, Bildungsstand)	Kontrollvariablen

3 Methodisches Vorgehen

Das dritte Kapitel begründet die Methodenwahl und beschreibt das geplante Vorgehen im Detail. Weiter werden die im konzeptionellen Modell aufgeführten Variablen operationalisiert, und es wird die Gestaltung des Fragebogens beschrieben.

3.1 Methodenwahl

Da die Ursache-Wirkungs-Beziehung zwischen Dark Patterns und des beobachteten Verhaltens untersucht werden soll, wurde als Forschungsmethode das Experiment gewählt (Eifler, 2014, S. 196).

Als Experiment wird eine systematische Beobachtungssituation bezeichnet, in der die unabhängigen Variablen variiert werden und ansonsten streng vergleichbare Untersuchungsbedingungen herrschen (Hussy et al., 2010, S. 114). Die Untersuchung wird online, anhand eines künstlich geschaffenen Szenarios, durchgeführt, und ist deshalb als Laborexperiment einzuordnen (Hussy et al., 2010, S. 135).

Das Experiment wird mit einer zufällig ausgewählten Experimental- und Kontrollgruppe als between-subject-design einer unabhängigen Stichprobe durchgeführt (Kuss et al., 2014, S. 179–180).

3.2 Forschungsdesign des Experiments

Das Experiment basiert auf einen A/B Testing von zwei Website-Versionen, auf denen die Befragung der Proband_innen stattfindet. Die Proband_innen werden randomisiert der Experimental- oder Kontrollgruppe zugeteilt (Bortz & Döring, 2006, S. 117).

Beim Einstieg wird bei beiden Versionen ein Cookie-Hinweis integriert, auf den der Proband reagieren muss, bevor mit der Befragung gestartet werden kann. Der Cookie-Hinweis wird möglichst nativ gestaltet und wird nicht explizit als Teil der Befragung deklariert, um möglichst realitätsnahe Reaktionen auf den Hinweis zu wecken. Dabei werden nur bei der Variante der Experimentalgruppe Dark Patterns auf dem Cookie-

Hinweis integriert. Der Kontrollgruppe wird ein Cookie-Hinweis frei von Dark Patterns präsentiert mit neutraler Ausgestaltung der Akzeptieren- und Ablehnen-Option.

Unabhängig von der Reaktion der Proband_innen auf den Cookie-Hinweis werden nur betriebsnotwendige Cookies gespeichert, die für den Rückschluss darauf, ob die Proband_innen die Sammlung der Cookies akzeptieren oder ablehnen, notwendig sind. Im Anschluss an die Interaktion mit dem Cookie-Hinweis, folgt der eigentliche Fragebogen zur Erhebung der restlichen Variablen. In der Abbildung 6 wird der Ablauf des Experiments visualisiert.

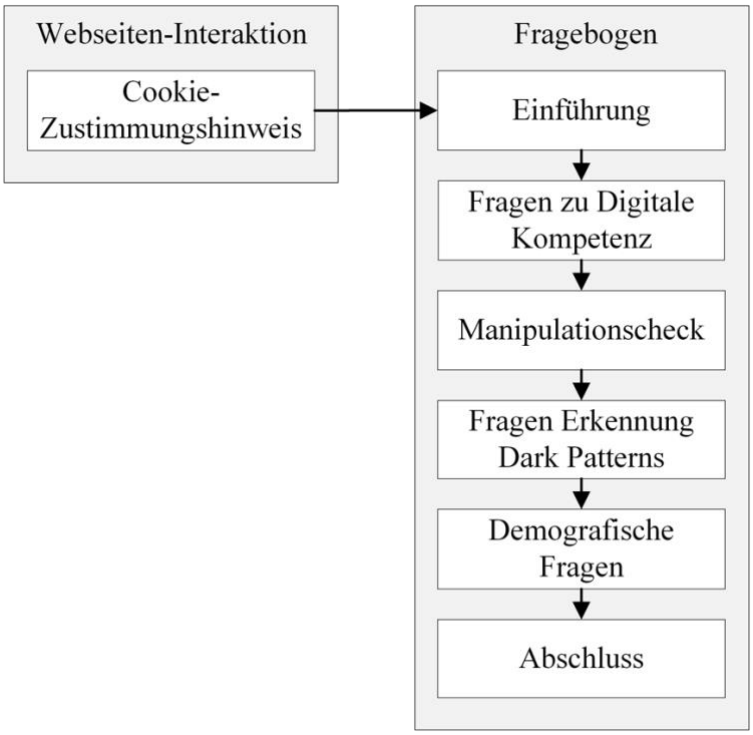


Abbildung 6: Ablauf des Experiments

Für die Erstellung des Fragebogens wird der Anbieter SurveyJS verwendet, da dessen Software die Einbindung des Fragebogens in eine Website und die Speicherung der Interaktion mit dem Cookie-Hinweis, welcher als natives Javascript-Element umgesetzt wurde, ermöglicht. Die Gestaltung und Umsetzung des Cookie-Zustimmungshinweis werden in Kapitel 3.4 genauer erläutert.

3.3 Operationalisierung

Im Rahmen der Operationalisierung werden theoretische Konzepte in messbare Variablen überführt (Döring & Bortz, 2016, S. 223). Dazu können entweder eigene Messinstrumente entwickelt oder auf vorhandene Messinstrumente zurückgegriffen werden (Döring & Bortz, 2016, S. 223).

Für die vorliegende Masterarbeit werden, wo vorhanden, bestehende Skalen verwendet. Die Übersetzung der englischen Originalskalen ins Deutsche erfolgt durch zwei Personen mit Muttersprache Deutsch und Sprachniveau Englisch C1-C2. Anschliessend werden die Ergebnisse der Übersetzung verglichen, sowie Uneinigkeiten diskutiert und bereinigt. Die Originalskalen mit finaler Übersetzung können in Anhang C eingesehen werden.

In der vorliegenden Arbeit wird mit Likert-Skalen, sowie mit einem Konstrukt mit einer bipolaren Ratingskala gearbeitet. Es werden für beide Skalen sieben Stufen gewählt, da in der Literatur zwischen fünf und sieben Stufen empfohlen werden (Döring & Bortz, 2016, S. 249). Die Likert-Skalierung wird auch als Technik der summierten Einschätzungen bezeichnet und findet in den Sozialwissenschaften breit Anwendung (Häder, 2019, S. 102). Bipolare Ratingskalen werden für die Beurteilung des subjektiven Empfindens einer Merkmalsausprägung verwendet und erhöhen durch die wechselseitige Definition die Präzision der Urteile (Döring & Bortz, 2016, S. 245).

In den folgenden Unterkapiteln wird die Operationalisierung der einzelnen Variablen beschrieben.

3.3.1 Digitale Kompetenz

Für die Erhebung der Digitalen Kompetenz wird aufgrund Kosten- und Zeitrestriktionen auf Selbsteinschätzung zurückgegriffen. Dazu wird das Konstrukt von Rodríguez-de-Dios et al. (2016) verwendet, in deren Skala, die im Kapitel 2.4.1 vorgestellten sechs Fertigkeitsdimensionen, abgefragt werden. Die Skala besteht insgesamt aus sechs Faktoren und 28 Items (Rodríguez-de-Dios et al., 2018, S. 195).

Im Gegensatz zum Vorgehen von Rodríguez-de-Dios et al. (2018) wird statt einer fünfstufigen Likert-Skala allerdings für mehr Granularität eine siebenstufige Likert-Skala eingesetzt (1= Stimme überhaupt nicht zu, 7 Stimme voll zu). Das Konstrukt enthält sieben Items zu technologischen Fertigkeiten, vier Items zu persönlicher Sicherheitskompetenz, fünf Fragen zu kritischer Analyse-Fertigkeit, vier Fragen zur Geräte-Sicherheitskompetenz, fünf Fragen zur Informationskompetenz und drei Fragen zu Kommunikationsfertigkeit. Sieben Items davon sind umgekehrt kodiert (reverse coded).

3.3.2 Erkennung von Dark Patterns

Im zweiten Teil der Befragung soll die Fähigkeit der User_innen, Dark Patterns zu erkennen, evaluiert werden.

Da im Bereich der Dark Patterns noch keine entsprechenden Konstrukte erarbeitet und validiert wurden, wird hier auf das Konstrukt zur Messung wahrgenommener Täuschung in der Werbung von Maddox (1982) zurückgegriffen. Das erwähnte Konstrukt wurde bereits von anderen Forschenden zur Untersuchung von Täuschungen im Internet eingesetzt und wird deshalb auch für die Anwendung auf Dark Patterns als geeignet erachtet (Grazioli & Jarvenpaa, 2000, S. 403).

Für die Beurteilung der wahrgenommenen Täuschung wird den Proband_innen der Cookie-Hinweis als Screenshot erneut präsentiert und sie werden gebeten, die Gestaltung desselben anhand drei Items zu bewerten. Die drei Items werden anhand einer bipolaren Sieben-Punkt-Matrix mit den Ausprägungen «klar» versus «irreführend», «vertrauenswürdig» versus «trügerisch» und «sachlich» versus «verzerrt» bewertet.

3.3.3 Zustimmung zu Cookies

Die Reaktion auf den Cookie-Zustimmungshinweis wird anhand der getroffenen Auswahl erhoben und entsprechend in der Datenbank gespeichert (0=«Alle ablehnen», 1= «Auswahl anpassen», 2=«Alle akzeptieren»).

3.3.4 Demografische Angaben

Für die Erhebung der höchsten abgeschlossenen Ausbildung, Beschäftigung und Art der Beschäftigung wird auf die Erhebungsmethode des Bundesamts für Statistik zurückgegriffen (Bundesamt für Statistik, 2022b). Die Art der Beschäftigung wird als offenes Textfeld und optionale Frage definiert. Weiter werden das Alter in Jahren, sowie das Geschlecht anhand der Optionen «weiblich», «männlich» oder «Nichtbinär/drittes Geschlecht» erhoben.

3.4 Gestaltung von Manipulation und Fragebogen

Im Folgenden wird genauer beschrieben wie die Manipulation, sprich die Cookie-Zustimmungshinweise, und der darauffolgende Fragebogen ausgestaltet werden.

3.4.1 Gestaltung der Manipulation

Die Ausgestaltung der Cookie-Zustimmungshinweise erfolgt in Anlehnung an die Standards der am weitesten verbreiteten Consent-Management-Anbieter wie Cookiebot, OneTrust oder QuantCast, um möglichst realitätsnahe Bedingungen für das Experiment zu schaffen (Nouwens et al., 2020, S. 5).

Um einen direkteren Vergleich der Cookie-Hinweis-Varianten zu ermöglichen, wird bei beiden Versionen jeweils die Option der Bestätigung als auch der Ablehnung angeboten. Die Formulierung des Cookie-Hinweises ist weitgehend auf die Standardformulierung von Cookiebot gestützt (Cookiebot, 2021). Analog zum Vorgehen von Grassl et al. (2021, S. 8) werden Elemente, die einen Vorteil für die User_innen suggerieren, entfernt, damit gemäss der Privacy Calculus Theory zu erwarten wäre, dass die User_innen den Cookie Request ablehnen (Smith et al., 2011, S. 1001).

Weiter werden die Erkenntnisse einer Studie von Utz et al. (2019) einbezogen, welche die User Interfaces eines Samples von 1'000 Cookie-Hinweisen hinsichtlich Variablen wie der Positionierung, des Textinhaltes, oder der Interaktionsmöglichkeit untersuchten. Auf Basis dieser Erkenntnisse wird die Platzierung am unteren Rand der Website gewählt. Die Einbettung der Cookie-Hinweise im Fragebogen können im Anhang B eingesehen werden.

In den Cookie-Hinweis der Experimentalgruppe werden die Dark Patterns «False Hierarchy» und «Preselection» inkorporiert. Dazu wird die Option «Alle zulassen» vorselektiert und durch Grösse und Farbe von der Option «Anpassen» beziehungsweise «Ablehnen» abgehoben. Weiter wird die Ablehnen-Option durch einen zusätzlichen Klick auf eine zweite Seite des Hinweises, erschwert (Nouwens et al., 2020, S. 8). Die Gestaltung der beiden Schritte des Cookie-Zustimmungshinweises der Experimentalgruppe können in Abbildung 7 und Abbildung 8 eingesehen werden.

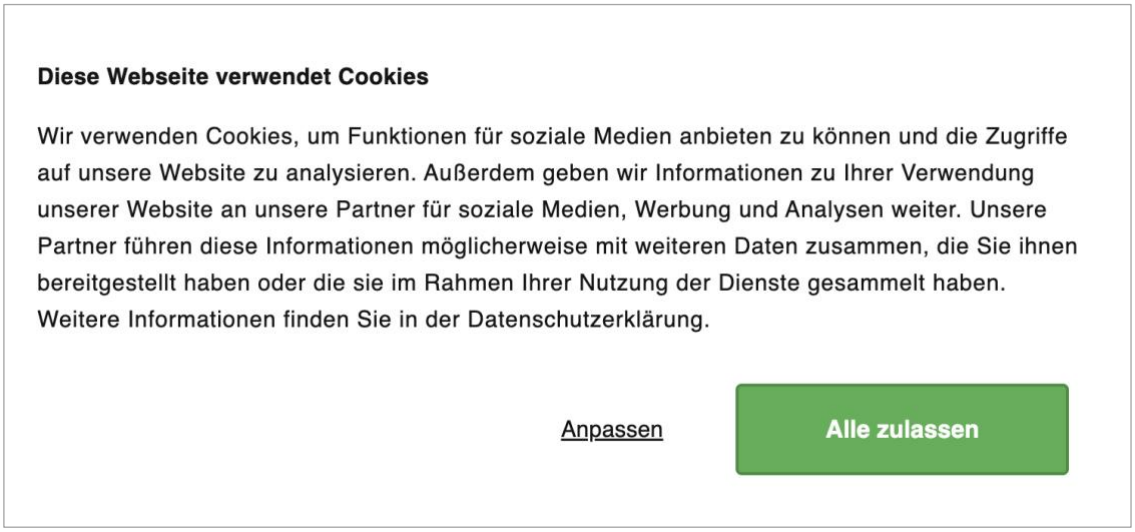


Abbildung 7: Cookie-Zustimmungshinweis mit Dark Pattern – Schritt eins

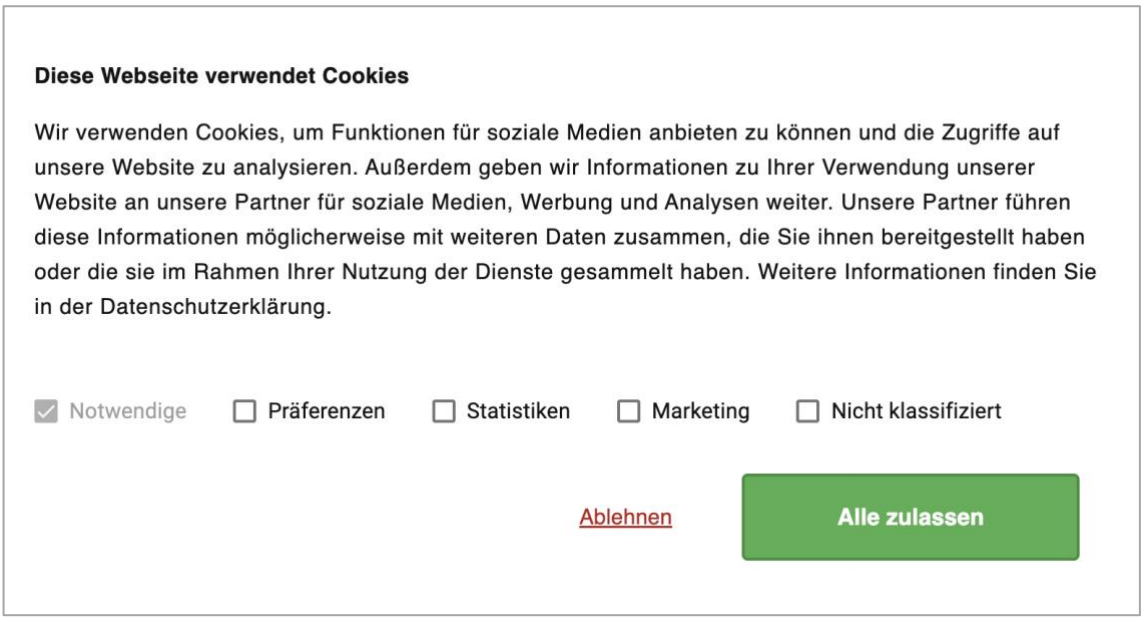


Abbildung 8: Cookie-Zustimmungshinweis mit Dark Pattern – Schritt zwei

In der Kontrollgruppe mit neutralem Cookie-Hinweis werden beide Optionen gestalterisch gleich gehalten und keine Vorauswahl getroffen. Die Texte sind identisch mit denjenigen der Experimentalgruppe. Die Gestaltung des Cookie-Zustimmungshinweises der Kontrollgruppe kann in der Abbildung 9 eingesehen werden.

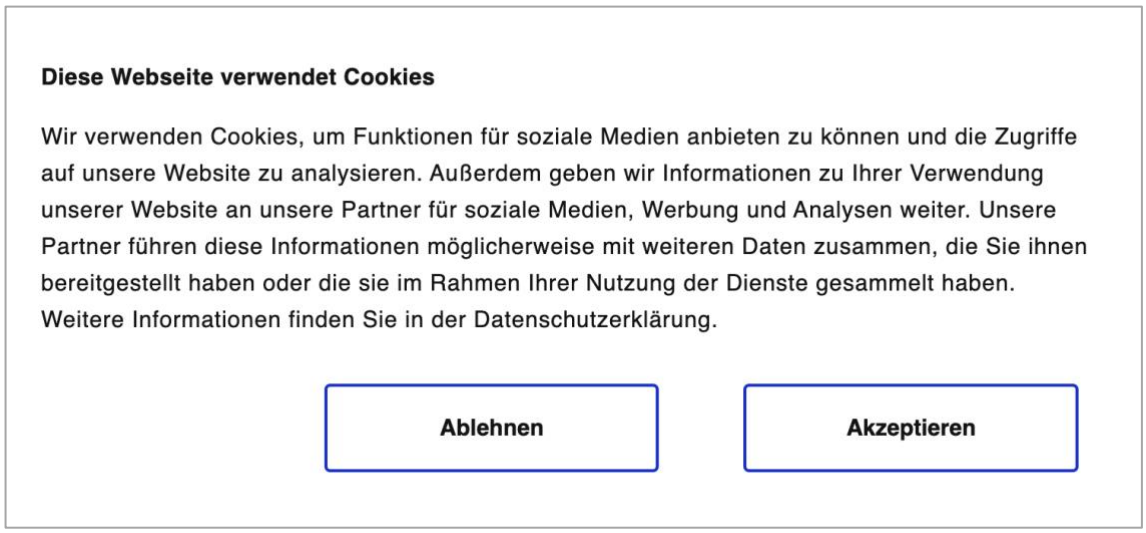


Abbildung 9: Cookie-Zustimmungshinweis ohne Dark Pattern

3.4.2 Gestaltung des Fragebogens

Anschliessend an die Interaktion mit der Manipulation wird der Fragebogen gestartet. Der Fragebogen beginnt mit einer Einführung, welche die Vorstellung des Themas, eine ungefähre Zeitangabe, sowie eine kurze Nennung des Erstellers umfasst. Als Thema der Befragung wurde die Thematik der Digitalen Kompetenz genannt, anstelle des eigentlichen Themas der Masterarbeit, um die Beantwortung nicht zu beeinflussen. Weiter wird die Teilnahme mit einer optionalen Gewinnspielteilnahme incentiviert, um die Teilnahmequote zu erhöhen.

Anschliessend an die Beantwortung der 28 Items zur Digitalen Kompetenz wird der Manipulationscheck durchgeführt. Im zweiteiligen Manipulationscheck wird geprüft, ob sich die Proband_innen an die Interaktion und den Inhalt des Cookie-Zustimmungshinweis erinnern, und ob die Manipulation der unabhängigen Variable damit erfolgreich war (Döring & Bortz, 2016, S. 117). Eine Rückwärtsnavigation innerhalb des Experiments wird nicht ermöglicht, um zu verhindern, dass die

Beantwortung der Fragen nachträglich überarbeitet wird. Anschliessend wird die Manipulation mittels Screenshots den Probanden erneut präsentiert und das Konstrukt zur Erkennung der Dark Patterns abgefragt.

Zuletzt werden die Fragen bezüglich Demographie gestellt, sowie eine Feedbackmöglichkeit zum Fragebogen geboten. Weiter kann in einem letzten Schritt durch Hinterlassung der E-Mailadresse am Wettbewerb teilgenommen werden, bevor den Proband_innen für die Teilnahme gedankt wird.

Ein Auszug des kompletten Fragebogens kann dem Anhang A entnommen werden.

3.5 Proband_innen

Für die Durchführung von Experimenten wird eine Gruppengrösse von 30 Proband_innen pro Gruppe empfohlen, womit für dieses Experiment total 60 Proband_innen vorausgesetzt werden (Huber et al., 2014, S. 29). Die Proband_innen werden initial über das Netzwerk der Autorin rekrutiert. Da eine Streuung der Digitalen Kompetenzen im Sample hinsichtlich des Untersuchungsziel essenziell ist, wird versucht eine Heterogenität hinsichtlich der Einflussfaktoren von Digitaler Kompetenz wie dem Alter oder dem Bildungsgrad zu erreichen. Aus diesem Grund wird das Schneeballverfahren eingesetzt, bei dem Mitglieder_innen aus der Population aufgefordert werden, weitere Untersuchungspersonen zu rekrutieren (Döring & Bortz, 2016, S. 308). Die Zuordnung der Proband_innen zur Experimental- oder Kontrollgruppe erfolgt nach dem Zufallsprinzip.

3.6 Mögliche Fehlerquellen

Im Folgenden werden mögliche Fehlerquellen beschrieben und aufgezeigt, wie diese bestmöglich limitiert werden. Die Aufführung der Fehlerquellen ist nicht als abschliessend zu betrachten.

Der Hawthorne-Effekt tritt auf, wenn Versuchspersonen ihr Verhalten verändern, weil sie im Wissen sind, dass sie untersucht werden und deshalb die Effekte nicht eindeutig auf das Treatment zurückgeführt werden können (Döring & Bortz, 2016, S. 101). Um den

Hawthorne-Effekt vorzubeugen, wird in der vorliegenden Untersuchung den Proband_innen das eigentliche Ziel der Untersuchung nicht offengelegt und die Cookie-Hinweise möglichst nativ eingebunden, damit diese nicht direkt als Teil der Untersuchung erkannt werden.

Bewertungsangst tritt auf, wenn Proband_innen ihr Verhalten aufgrund der Angst vor einer negativen Bewertung verändern (Döring & Bortz, 2016, S. 101). Ähnliche Auswirkungen hat der Effekt der «Sozialen Erwünschtheit», wobei die Beantwortung aufgrund der Furcht von sozialer Verurteilung verfälscht wird (Döring & Bortz, 2016, S. 437). In der vorliegenden Arbeit könnten die genannten Effekte bei der Selbsteinschätzung der Digitalen Kompetenz auftreten. Dieser Fehlerquelle wird Rechnung getragen, indem auf Anonymität in der Auswertung der Befragung hingewiesen wird.

Als weitere mögliche Fehlerquelle wurde der Selektionseffekt identifiziert. Selektionseffekte treten auf, wenn sich die Personen der Untersuchungsgruppen hinsichtlich relevanter Charakteristika voneinander unterscheiden (Döring & Bortz, 2016, S. 101). Um Selektionseffekte vorzubeugen, erfolgt die Zuteilung zur Experimental- versus Kontrollgruppe randomisiert.

3.7 Pretest

Bevor mit der Durchführung des Experiments gestartet werden kann, wird ein Pretest empfohlen, um allfällige Mängel identifizieren und korrigieren zu können (Baur & Blasius, 2014, S. 50).

Der Pretest wurde mit fünf Personen aus der Zielgruppe anhand der Technik des lauten Denkens, sowie der Nachfragetechnik durchgeführt (Weichbold, 2014, S. 301).

Basierend auf den Pretest-Ergebnissen wurden folgende Punkte überarbeitet:

- In der Frage «Ich weiss, wie ich eine Webseite, die mir gefällt, mit einem Lesezeichen versehe, damit ich sie mir später ansehen kann.» wurde «oder als

Favorit speichere», ergänzt, da identifiziert wurde, dass «Lesezeichen» nicht von allen Proband_innen verstanden wurde und die Funktion bei einigen Browsern mit «als Favorit speichern», bezeichnet wird.

- In der Formulierung der Frage zur Erkennung der Dark Patterns («Bitte bewerten Sie die Gestaltung des abgebildeten Cookie-Hinweises an der folgenden Skala.») wurde der Zusatz «grafischen» ergänzt, da die Proband_innen des Pretests ihr Urteil fast ausschliesslich anhand der textlichen Formulierung fällten.

- Im Item «Ich weiss, wie ich Informationen, die ich online gefunden habe, herunterladen kann.» wurde ein Beispiel ergänzt, da nicht von allen Proband_innen verstanden wurde, auf was sich «Informationen» bezieht.

- Es wurden einige Device-spezifische Optimierungen hinsichtlich der Darstellung des Cookie-Zustimmungshinweises sowie des Fragebogens vorgenommen.

Die anderen Fragen wurden von den Proband_innen als verständlich beurteilt und es wurden keine weiteren Mängel identifiziert. Die durchschnittliche Bearbeitungsdauer betrug sieben Minuten, was als vertretbar beurteilt wurde.

4 Resultate

Im folgenden Kapitel werden das Experiment ausgewertet und die Resultate werden vorgestellt. Einleitend wird beschrieben, wie die Daten aufbereitet wurden, und es wird die Stichprobe beschrieben.

4.1 Aufbereitung der Daten

Im Rahmen der Datenaufbereitung wurde der Datensatz auf Vollständigkeit und Fehler überprüft, und es wurden Rekodierungen vorgenommen (Kuss et al., 2014, S. 150). Die Beantwortungsdauer aller Proband_innen lag über vier Minuten, was als akzeptabel eingeordnet wurde. Ein Fall wurde aufgrund des Feedbacks, dass die Fragen fehlerhaft angezeigt wurden, ausgeschlossen, und ein weiterer aufgrund Auffälligkeiten bei der Beantwortung reverse-codierter Fragen, was auf eine unaufmerksame Beantwortung der Befragung hinweist.

Weiter wurden für die Multi-Item-Skalen zu Digitaler Kompetenz inklusive deren Subdimensionen, sowie für das Konstrukt zur Erkennung von Dark Patterns die Mittelwerte berechnet. Die Variable «Digitale Kompetenz» berechnete sich durch den Mittelwert der Mittelwerte der sechs Subdimensions-Variablen.

Bei der Interaktion mit dem Cookie-Zustimmungshinweis wurde in der Experimentalgruppe aufgezeichnet, ob die Option «Alle akzeptieren» versus «Auswahl erlauben» oder «Ablehnen» gewählt wurde. Weiter wurde bei der Option «Auswahl erlauben», welche die Sammlung der Cookies einschränkt, aber nicht komplett ablehnt, erfasst, bei welchen Parametern (bspw. Ablehnung Cookies für Marketingzwecke) eine Anpassung vorgenommen wurde. Beim Cookie-Zustimmungshinweis der Kontrollgruppe konnten die Nutzer_innen keine Anpassungen vornehmen, weshalb lediglich die Reaktion auf die beiden Buttons «Akzeptieren» und «Ablehnen» registriert wurde.

Im Rahmen der Rekodierung wurde die Reaktion «Auswahl erlauben» als eine Ablehnung der Cookies gewertet, da es sich um eine Einschränkung der Cookies handelt, die nur durch Mehraufwand via mehrere Klicks, erreicht werden konnte.

4.2 Beschreibung der Stichprobe

Insgesamt haben 103 Personen an der Onlinebefragung teilgenommen. Nach der Bereinigung um die zwei oben genannten Fälle, verlieben 101 Proband_innen, welche sich zu 44.6 Prozent auf die Experimental- und 55.4 Prozent auf die Kontrollgruppe aufteilten. Der Unterschied in den Gruppengrössen ist als nicht signifikant einzustufen (Exakter Binomialtest, zweiseitig, p = .320, n = 101).

Es haben 52.5 Prozent Frauen und 47.5 Prozent Männer an der Befragung teilgenommen. Die Altersspanne reichte von 22 bis 79 Jahren bei einem Durchschnittsalter von 42 Jahren und einem Median von 34 Jahren (MW=42.04, M=34, SD=16.23). Die Verteilung der Proband_innen nach Altersgruppen kann der Abbildung 10 entnommen werden. Über die Hälfte (54.5 Prozent) der Proband_innen waren zwischen 20 – 39 Jahre alt.

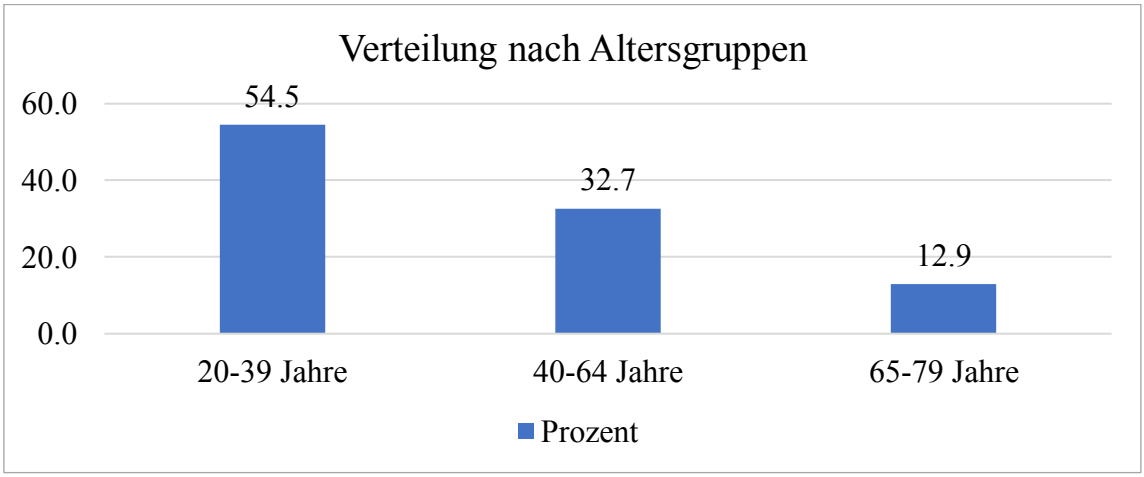


Abbildung 10: Verteilung der Proband_innen nach Altersgruppen

Der Grossteil der Proband_innen verfügte über einen Hochschulabschluss (42.6 Prozent). 25.7 Prozent hatten eine höhere Berufsbildung, 22.8 Prozent eine Berufslehre und 7.9 Prozent eine Maturität absolviert. Die Angabe einer Probandin (1 Prozent), konnte keiner der genannten Kategorien zugeordnet werden. 71.3 Prozent gaben an hauptsächlich erwerbstätig zu sein. 11.9 Prozent sind in AHV-Rente, 10.9 Prozent in schulischer

Ausbildung oder im Studium, 4.0 Prozent in der Kinderbetreuung/Haushalt/Familie tätig, sowie 2.0 Prozent sind in IV-Rente.

Für die Prüfung soziodemografischer Unterschiede zwischen der Experimental- und Kontrollgruppe wurden Pearson-Chi-Quadrat-Tests und t-Tests eingesetzt.
Es lagen keine signifikanten Unterschiede zwischen den Gruppen hinsichtlich des Geschlechts (Chi-Quadrat(1)= 1.558, p = .212), und hinsichtlich des Alters (t(99)= -.972, p= .334) vor.

Die Spanne der Digitalen Kompetenz reichte von 1.5 bis 7.0. Der Mittelwert lag bei 5.2 und einem Median von 5.5 (MW=5.200, M=5.47, SD=1.27). Eine Verteilung der Digitalen Kompetenz nach Altersgruppe kann in der Abbildung 11 eingesehen werden. Die Digitale Kompetenz war nicht normalverteilt und rechtsschief (Kolmogorov-Smirnov = $p < .001$; Shapiro-Wilk = $p < .001$). Es lagen keine signifikanten Unterschiede zwischen den Gruppen hinsichtlich der Digitalen Kompetenz vor (exakter Mann-Whitney-*U*-Test: $U = 1253.500$, $p = .965$).

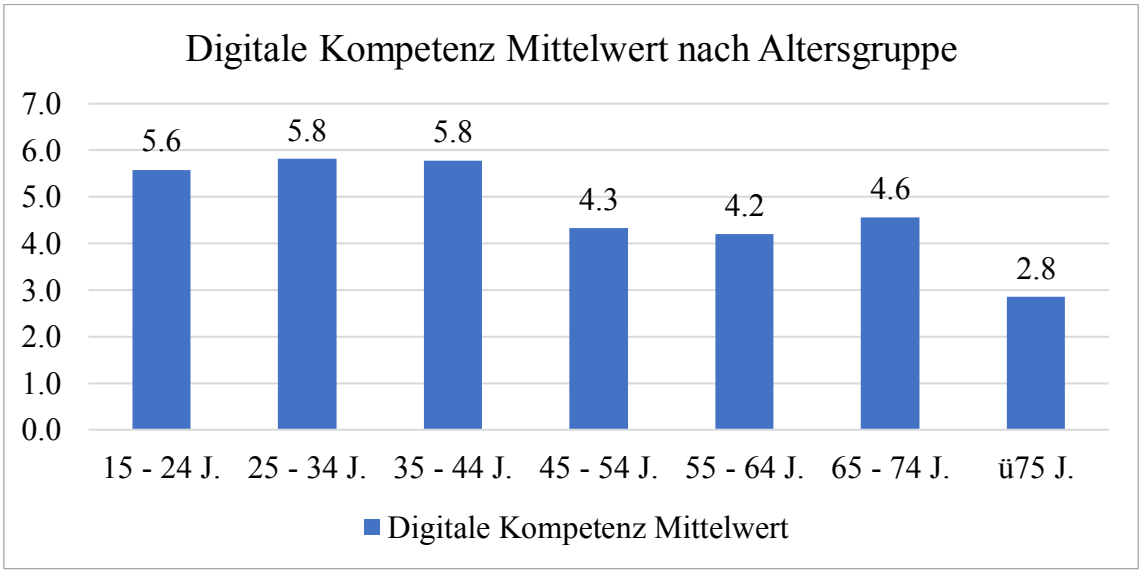


Abbildung 11: Digitale Kompetenz Mittelwert nach Altersgruppe

Weitere Informationen zur Beschreibung der Stichprobe können dem Anhang D entnommen werden.

4.3 Manipulationscheck

Der Manipulationscheck wird bei Experimenten in der Regel durchgeführt, um sicherzustellen, dass die Ausprägungen der abhängigen Variablen auf die unterschiedlichen Faktorstufen der unabhängigen Variablen zurückzuführen sind (Backhaus et al., 2016, S. 210). In der Forschung ist es dabei gängig, dass Proband_innen, welche den Manipulationscheck aufgrund einer fehlerhaften Antwort nicht bestehen, aus dem Sample ausgeschlossen werden (Oppenheimer et al., 2009, S. 871).

In der vorliegenden Studie ist die Interaktion mit dem Cookie-Zustimmungshinweis als Manipulation zu werten. Da es für Cookie-Zustimmungshinweise charakteristisch ist, dass diese unbewusst und unaufmerksam beantwortet werden (Utz et al., 2019, S. 974), wurden entgegen der gängigen Praxis die Proband_innen, welche den Manipulationscheck nicht bestanden, in der Auswertung nicht ausgeschlossen.

Tabelle 5 ist zu entnehmen, dass der Grossteil der Proband_innen, (75.2 Prozent) die korrekte Antwort trafen und 22.8 Prozent sich nicht daran erinnern konnte, was der Inhalt des Pop-ups war, das zu Beginn der Befragung eingeblendet wurde. Lediglich zwei Proband_innen, trafen eine falsche Auswahl.

Tabelle 5: Verteilung Beantwortung Manipulationscheck 1 – Frage nach Inhalt Pop-up

Antwort	Anzahl	Prozent
Sammlung von Cookies	76	75.2
«Weiss nicht»	23	22.8
Newsletter-Anmeldung	1	1.0
Videoaufnahme der Session	1	1.0

Der Manipulationscheck 2 prüfte, ob sich die Proband_innen, an ihre Reaktion auf den Cookie-Zustimmungshinweis erinnerten. Wie Tabelle 6 zu entnehmen ist, gaben 15.8 Prozent eine falsche Antwort, und 12.9 Prozent konnten sich nicht erinnern.

Tabelle 6: Verteilung Beantwortung Manipulationscheck 2

Antwort	Anzahl	Prozent
Korrekte Antwort	72	71.3
Falschangabe	16	15.8
«Weiss nicht»	13	12.9

Diejenigen Nutzer_innen, welche die Sammlung der Cookies abgelehnt oder eingeschränkt hatten, konnten sich, wie in Abbildung 12 ersichtlich, besser an die getätigte Antwort erinnern als diejenigen, welche die Cookies akzeptierten. Unter den Proband_innen, die die Cookies akzeptierten, konnten sich nur 67.8 Prozent korrekt an die getätigte Antwort erinnern.

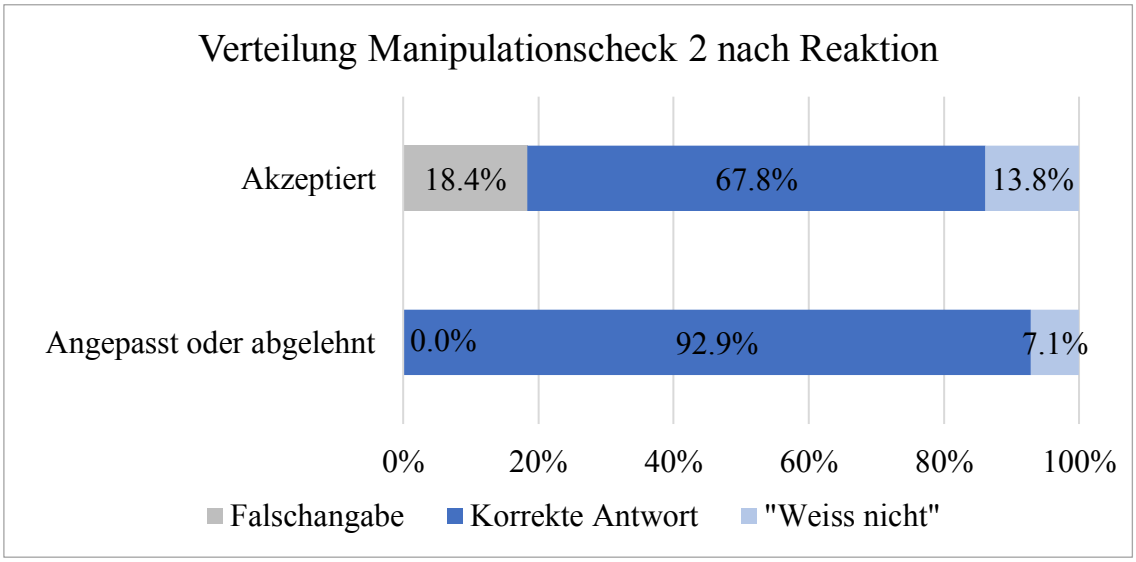


Abbildung 12: Beantwortung des Manipulationscheck 2 nach Reaktion

4.4 Reliabilität der Skalen

Die häufigste Methode zur Bestimmung der Reliabilität ist die Berechnung des Cronbachs-Alpha-Koeffizienten (Döring & Bortz, 2016, S. 443). Der α-Koeffizient misst die Korrelation der einzelnen Items einer Skala und somit deren interne Konsistenz (Kuss et al., 2014, S. 109). Gemäss einer Metaanalyse von Peterson (1994, S. 388) sollte der Cronbachs-Alpha-Koeffizient über einem Wert von 0.7 liegen.

Tabelle 7 kann entnommen werden, dass alle Konstrukte, bis auf die Kommunikationsfertigkeit, ein Cronbach's Alpha über 0.7 aufwiesen. Im Konstrukt «Kommunikationsfertigkeit» wurde das Item «coms_3» entfernt, wodurch das Cronbach's Alpha auf einen Wert von .534 anstieg, was als schwach, aber verwendbar zu beurteilen ist (George & Mallery, 2003, S. 231).

Tabelle 7: Reliabilität der Konstrukte

Konstrukt	Enthaltene Items	Cronbachs Alpha
Digitale Kompetenz		
Technologische Fertigkeiten	ts_1, ts_2, ts_3, ts_4, ts_5, ts_6, ts_7	.861
Persönliche Sicherheitskompetenz	pss_1, pss_2, pss_3, pss_4	.772
Kritische Analyse-Fertigkeit	cs_1, cs_2, cs_3, cs_4, cs_5	.943
Geräte-Sicherheitskompetenz	dss_1, dss_2, dss_3, dss_4	.727
Informationskompetenz	is_1, is_2, is_3, is_4, is_5	.817
Kommunikationsfertigkeit	coms_1, coms_2, coms_3	.275
Erkennung Dark Patterns		
Wahrgenommene Täuschung	de_1, de_2, de_3	.744

4.5 Konstruktvalidität

Zur Überprüfung der Konstruktvalidität wurde eine konfirmatorische Faktorenanalyse in der Statistiksoftware R mit dem darin enthaltenen Package «lavaan» durchgeführt.

Dabei sollten der Comparative Fit Index (CFI) über dem Grenzwert von 0.9 (Bentler, 1990), die Standardized Root Mean Squared Residuals (SRMR) unter dem Grenzwert von 0.8 (Hu & Bentler, 1999), sowie der Root Mean Square Error of Approximation

(RMSEA) zwischen 0.05 und 0.08 liegen (Fabrigar et al., 1999), um die Übereinstimmung des hypothetischen Modells mit den beobachteten Daten als gut zu beurteilen.

Das Modell erreichte die genannten Grenzwerte (SRMR = 0.069, RMSEA = 0.066, CFI = 0.904) und ist damit als akzeptabel zu bewerten. Weiter waren alle Faktorladungen auf einem Niveau von $p < .003$ signifikant. Der Output der konfirmatorischen Faktorenanalyse kann im Anhang E eingesehen werden.

4.6 Prüfung der Hypothesen

4.6.1 H1: Dark Pattern – Zustimmung zu den Cookies

Die Hypothese 1 postulierte, dass ein Zusammenhang zwischen dem Einsatz von Dark Patterns und der Zustimmung zum Cookie-Hinweis besteht.

Wie der Tabelle 8 entnommen werden kann, haben insgesamt 86.1 Prozent der Proband_innen die Sammlung der Cookies akzeptiert und 13.9 Prozent haben sie abgelehnt. In der Experimentalgruppe, unter Einsatz von Dark Patterns, lag die Zustimmung zu den Cookies um 9.0 Prozent höher als in der Kontrollgruppe ohne Dark Patterns. Die Unterschiede von Akzeptanz zu Ablehnung sind sowohl in der Experimentalgruppe (Exakter Binomialtest, zweiseitig, $p < .001$ $n = 45$) als auch in der Kontrollgruppe (Exakter Binomialtest, zweiseitig, $p < .001$ $n = 56$) als signifikant einzustufen.

Tabelle 8: Kreuztabelle Gruppe - Reaktion auf Cookie-Zustimmungshinweis

Gruppe		Cookies abgelehnt	Cookies akzeptiert	Gesamt
Experimental-gruppe	Anzahl	4	41	45
	% von Experimentalgruppe	8.9%	91.1%	100.0%
Kontroll-gruppe	Anzahl	10	46	56
	% von Kontrollgruppe	17.9%	82.1%	100.0%

Gesamt	Gesamt	14	87	101
	% von Gesamt	13.9%	86.1%	100.0%

Für die Prüfung des Zusamenhangs zwischen Dark Patterns und der und der Zustimmung zu den Cookies wurde der Pearson Chi-Quadrat-Test durchgeführt. Aufgrund der Stichprobengrösse und dem Freiheitsgrad von eins wurde die Korrektur nach Yates verwendet (Universität Zürich, 2022c). Der Einsatz von Dark Patterns und die Zustimmung zu den Cookies dabei in keinem signifikanten Zusammenhang (Chi-Quadrat(1) = 1.014, p = .314, n = 101). Damit muss die Hypothese 1 des direkten Effekts von Dark Patterns auf die Zustimmung zu den Cookies, verworfen werden.

4.6.2 H2: Moderierender Effekt der Erkennung von Dark Patterns auf deren Wirkung

Die Hypothese 2 postulierte, dass die Erkennung der Dark Patterns die Wirkung von Dark Patterns auf die Zustimmung zu den Cookies mindert.

Während die Experimentalgruppe den Cookie-Zustimmungshinweis mit Dark Patterns anhand der Skala zur wahrgenommenen Täuschung beurteilte, tat die Kontrollgruppe dasselbe anhand eines Cookie-Zustimmungshinweis frei von grafischen Manipulationselementen. Demnach müssten sich die Mittelwerte der beiden Gruppen signifikant unterscheiden. Die deskriptive Statistik zu den resultierten Werten kann Tabelle 9 entnommen werden.

Der Kolmogorov-Smirnov-Test als auch der Shapiro-Wilk-Test auf Normalverteilung waren signifikant ($p < .05$). Zur Überprüfung auf Unterschiede im Bereich der Dark-Pattern-Erkennung zwischen der Experimental- und Kontrollgruppe wurde deshalb der Mann-Whitney-U-Test eingesetzt, da die Prämisse der Normalverteilung für den t-Tests nicht erfüllt wurde (Universität Zürich, 2022a; Universität Zürich, 2022b). Dabei wies die Experimentalgruppe (Median=3, SD=1.6) keine signifikant höheren Werte als die Kontrollgruppe (Median=3, SD=1.3) auf (exakter Mann-Whitney-*U*-Test (ein-seitig): $U = 1218.500$, $p = .776$).

Tabelle 9: Deskriptive Statistik Erkennung von Dark Patterns

Gruppe	n	Mittelwert	Median	Standardabweichung
Experimentalgruppe	45	3.18	3	1.6
Kontrollgruppe	56	3.01	3	1.3

Der Moderationseffekt der Hypothese 2 wurde mittels der SPSS-Erweiterung PROCESS v4.1, «Model 1» von Hayes untersucht. Wie der Tabelle 10 entnommen werden kann, wurde kein signifikanter Moderationseffekt beobachtet (p=.9194), womit die Hypothese 2 verworfen wurde.

Tabelle 10: Moderationsanalyse Dark Pattern Erkennung

Prädiktor	β	p
Konstante	1.5358	.0000
Dark Pattern (Gruppe)	.7951	.2098
Dark Pattern Erkennung	.0803	.7657
Interaktion	.0450	.9194

4.6.3 H3a: Digitale Kompetenz – Erkennung von Dark Patterns

Die Hypothese 3a postulierte, dass sich Digitale Kompetenz positiv auf die Fähigkeit, Dark Patterns zu erkennen, auswirkt.

Da nur in der Experimentalgruppe Dark Patterns zum Einsatz kamen, wurde der Effekt nur anhand der Experimentalgruppe untersucht. Für die Prüfung der Hypothese wurde eine einfache lineare Regressionsanalyse eingesetzt, da der Zusammenhang zweier intervallskalierter Variablen untersucht werden sollte (Universität Zürich, 2022a).

Die Modellzusammenfassung der linearen Regressionsanalyse kann der Tabelle 11 entnommen werden. Das Resultat der linearen Regressionsanalyse fiel nicht signifikant aus (p =.921). Die digitale Kompetenz leistet keinen Beitrag zur Erklärung der Varianz

der Erkennung von Dark Patterns ($F(1, 43) = .010$, $p = .921$). Die Hypothese 3a wurde deshalb abgelehnt.

Tabelle 11: Modellzusammenfassung des Regressionsmodells Digitale Kompetenz - Dark Pattern Erkennung

Modell	R	R^2	Korrigiertes R^2	Standardfehler des Schätzers
1	.015	.000	-.023	1.61779

4.6.4 H3b: Moderierender Effekt der Digitalen Kompetenz auf die Wirkung von Dark Patterns

Die Hypothese 3b postulierte, dass Digitale Kompetenz die Wirkung von Dark Patterns auf die Zustimmung zu den Cookies mindert.

In der Moderationsanalyse mit PROCESS «Model 1» wurde kein signifikanter Moderationseffekt beobachtet (p=.3702). Die Hypothese 3b wurde aus diesem Grund abgelehnt. Die Modellzusammenfassung der Moderationsanalyse kann der Tabelle 12 entnommen werden.

Tabelle 12: Moderationsanalyse Digitale Kompetenz

Prädiktor	β	p
Konstante	1.5247	.0000
Dark Pattern (Gruppe)	.8632	.1879
Digitale Kompetenz	-0.0456	.8718
Interaktion	.5530	.3702

4.6.5 H3c: Digitale Kompetenz – Zustimmung zum Cookie-Hinweis

Die Hypothese H3c postulierte, dass die Digitale Kompetenz in einem negativen Zusammenhang mit der Zustimmung zu den Cookies steht.

Zur Untersuchung des Zusammenhangs zwischen der metrischen, abhängigen Variabel «Digitale Kompetenz» und der binär skalierten Variable «Zustimmung zu den Cookies», wurde eine logistische Regressionsanalyse eingesetzt. Das Modell der logistischen Regression fiel nicht signifikant aus (Chi-Quadrat(1) = .118, p = .731, n = 101). Auch bei Dichotomisierung der Digitalen Kompetenz mittels Mediansplit wurden keine Unterschiede hinsichtlich der Zustimmung zu den Cookies festgestellt (Chi-Quadrat(1) = .000, p = 1.000, n = 101). Die Hypothese H3c wurde deshalb verworfen.

Tabelle 13: Kreuztabelle Digitale Kompetenz dichotomisiert – Reaktion auf Cookie-Zustimmungshinweis

Digitale Kompetenz		Cookies abgelehnt	Cookies akzeptiert	Gesamt
Tiefe Digitale Kompetenz	Anzahl	7	43	50
	% von tiefe Digitale Kompetenz	14.0%	86.0%	100.0%
Hohe Digitale Kompetenz	Anzahl	7	44	51
	% von hohe Digitale Kompetenz	7.1 %	43.9%	100.0%
Gesamt	Gesamt	14	87	101
	% von Gesamt	13.9%	86.1%	100.0%

4.6.6 Zusammenfassung der Hypothesenprüfung

Abschliessend werden die Resultate der einzelnen Hypothesenprüfungen in der Tabelle 14 zusammenfassend darstellt. In der Prüfung der Hypothesen wurden keine signifikanten Resultate gemessen, womit alle Hypothesen abgelehnt wurden.

Tabelle 14: Zusammenfassung der Hypothesenprüfung

Hypothese	Resultat
H1: Der Einsatz von Dark Patterns wirkt sich positiv auf die Zustimmung zu den Cookies aus.	abgelehnt
H2: Die Erkennung des Dark Patterns mindert die Wirkung von Dark Patterns auf die Zustimmung zu den Cookies.	abgelehnt
H3a: Digitale Kompetenz wirkt sich positiv auf die Fähigkeit Dark Patterns zu erkennen aus.	abgelehnt
H3b: Digitale Kompetenz mindert die Auswirkung von Dark Patterns auf die Zustimmung zu den Cookies.	abgelehnt
H3c: Digitale Kompetenz wirkt sich negativ auf die die Zustimmung zu den Cookies aus.	abgelehnt

4.7 Gütekriterien

Die Wissenschaftlichkeit empirischer Untersuchungen wird anhand von Gütekriterien geprüft (Hussy et al., 2010, S. 22).
Im Rahmen von Experimenten wird die Güte anhand der drei Hauptkriterien Objektivität, Reliabilität und Validität dargestellt (Himme, 2009, S. 485). Im Folgenden wird erläutert, wie ebendiese Kriterien in der vorliegenden Thesis sichergestellt wurden.

4.7.1 Objektivität

Objektivität beschreibt, dass wenn verschiedene Personen eine Messung unabhängig voneinander durchführen, diese zu den gleichen Ergebnissen gelangen (Himme, 2009, S. 495). Gemäss Hussy et al. (2010, S. 22) kann Objektivität hauptsächlich durch eine Standardisierung von Durchführung, Auswertung und Interpretation der Untersuchung erreicht werden.

In der Masterarbeit wurde die Onlinebefragung als Methodik gewählt, womit eine Beeinflussung durch die Untersuchungsleitung minimiert und somit die Durchführungsobjektivität gewährleistet wurde (Himme, 2009, S. 495). Die

Auswertungsobjektivität wurde durch den Einsatz geprüfter Skalen und standardisierter statistischer Auswertungsmethoden sichergestellt (Himme, 2009, S. 495). Die Interpretationsobjektivität kann nicht abschliessend beurteilt werden, da kein zweiter Messvorgang durch eine unterschiedliche Untersuchungsleitung durchgeführt wurde (Berekoven et al., 2009, S. 80).

4.7.2 Reliabilität

Die Reliabilität liegt vor, wenn Messwerte präzis, stabil und somit reproduzierbar sind (Berekoven et al., 2009, S. 81).

Um dies zu gewährleisten, wurde weitgehend auf bestehende, geprüfte Skalen zurückgegriffen. Weiter wurde die Reliabilität der Multi-Item-Skalen mittels Cronbachs Alpha, dem Mass für interne Konsistenz, geprüft und in Kapitel 4.4 für die jeweiligen Konstrukte ausgewiesen (Kuss et al., 2014, S. 109). In der Skala zur Messung der Digitalen Kompetenz wurde ein Item aufgrund eines ungenügenden Cronbachs Alpha-Werts ausgeschlossen.

4.7.3 Interne und externe Validität

Das dritte Gütekriterium der Validität ist bei Experimenten von besonderer Bedeutung (Hussy et al., 2010, S. 131). Die interne Validität liegt vor, wenn Veränderungen in der abhängigen Variabel, einzig auf eine Variation der unabhängigen Variable zurückgeführt und somit der Einfluss von Störvariablen ausgeschlossen werden kann (Himme, 2009, S. 491).

Bei einer Onlinebefragung können individuelle Gegebenheiten und damit Störvariablen weniger stark kontrolliert werden als bei einer Durchführung unter Laborbedingungen (Hussy et al., 2010, S. 135). Der internen Validität wurde allerdings versucht durch eine randomisierte Zuteilung der Proband_innen zur Experimental- und Kontrollgruppe, sowie durch eine Verschweigung des eigentlichen Untersuchungsgegenstandes und damit Verhinderung des Treatment-Effekts, Rechnung getragen (Kuss et al., 2014, S. 187–188). Externe Validität ist gegeben, wenn Untersuchungsergebnisse generalisierbar sind und somit von der betrachteten Stichprobe auf die Grundgesamtheit übertragen werden

können (Berekoven et al., 2009, S. 82). In der vorliegenden Arbeit ist die externe Validität aufgrund der (mittels Onlinebefragung) ungenügenden Erreichbarkeit bestimmter Bevölkerungsschichten und wegen der fehlenden Möglichkeit der Ziehung einer reinen Zufallsstichprobe als eingeschränkt zu beurteilen (Treiblmaier, 2010, S. 11).

4.8 Explorative Untersuchungsergebnisse

Ergänzend zur Prüfung der Hypothesen wurden Zusammenhänge basierend auf den erhobenen Daten explorativ untersucht. Das nachfolgende Kapitel beschreibt die wichtigsten Erkenntnisse.

4.8.1 Einfluss soziodemografischer Faktoren auf die Zustimmung zu den Cookies

Der Zusammenhang zwischen soziodemografischen Faktoren und der Zustimmung zu den Cookies wurde mittels Pearson-Chi-Quadrat-Tests, sowie logistischer Regressions-analysen untersucht. Dabei wurden keine signifikanten Unterschiede und Zusammenhänge festgestellt werden. Die Resultate können in Anhang E eingesehen werden.

4.8.2 Erinnerung an Beantwortung des Cookie-Zustimmungshinweises

Ergänzend zur Reaktion auf den Cookie-Zustimmungshinweis wurde die Beantwortung der Manipulationschecks hinzugezogen, um mögliche Zusammenhänge zu eruieren. Dabei wurde geprüft, ob ein Zusammenhang zwischen dem Einsatz des Dark Patterns und einer fehlerhaften Antwort auf den Manipulationscheck zwei besteht, der prüfte, ob sich die Proband_innen an ihre Reaktion auf den Cookie-Zustimmungshinweis erinnerten.

Da die erwarteten Zellhäufigkeiten in drei Zellen unter fünf lagen, wurde der exakte Test nach Fisher anstelle des klassischen Pearson-Chi-Quadrat-Tests eingesetzt (Universität Zürich, 2022c). Dabei zeigte sich ein signifikanter Zusammenhang zwischen dem Einsatz von Dark Patterns und der Erinnerung an die getätigte Reaktion (Exakter Test nach Fisher (2)= 13.527, p =<.001, n = 76). Die Resultate sind in der Tabelle 15 ersichtlich. Für diese Analyse wurden nur die Proband_innen betrachtet, welche den ersten Manipulationscheck bestanden, welcher den Inhalt des gezeigten Pop-ups erfragte und

damit eine Voraussetzung für die Beantwortung des zweiten Manipulationscheck darstellte. Dadurch wurden 25 Proband_innen ausgeschlossen.

Tabelle 15: Kreuztabelle Einsatz Dark Pattern - Beantwortung Manipulationscheck 2

Gruppe		Falsch-angabe	Korrekte Angabe	«Weiss nicht»	Gesamt
Experimental-gruppe	Anzahl	10	22	1	33
	% von Experimental-gruppe	30.3%	66.7%	3.0%	100.0%
Kontroll-gruppe	Anzahl	1	42	0	43
	% von Kontrollgruppe	2.3%	97.7%	0.0%	100.0%
Gesamt	Gesamt	11	64	1	76
	% von Gesamt	14.5%	84.2%	1.3%	100.0%

Aufbauend auf diesen Resultaten wurde analog des Conceptual Models auch ein direkter Effekt der Digitalen Kompetenz auf den Manipulationscheck zwei, sowie ein möglicher Moderatoreffekt der Digitalen Kompetenz geprüft. Dabei konnten keine signifikanten Effekte festgestellt werden. Die Resultate können in Anhang E eingesehen werden.

5 Diskussion

Das Ziel der Arbeit war es, personenbezogene Faktoren, welche die Wirkung von Dark Patterns moderieren und damit gewisse Personen vulnerabler für Dark Patterns machen, zu identifizieren. Dazu wurde ein Experiment durchgeführt, wobei der Einsatz von Dark Patterns auf einem Cookie-Zustimmungshinweis geprüft wurde.

Im folgenden Kapitel werden die Ergebnisse der Untersuchung kritisch gewürdigt und mit der relevanten Literatur in Verbindung gebracht. In einem zweiten Schritt werden Implikationen für Theorie und Praxis, sowie Limitationen der Arbeit aufgezeigt.

5.1 Würdigung der Resultate

Im Folgenden werden die wichtigsten Resultate zusammengefasst und in den Kontext der relevanten Literatur gestellt.

5.1.1 Direkter Effekt von Dark Patterns auf die Zustimmung zu Cookies

Sowohl in der Experimentalgruppe, unter Einsatz von Dark Patterns, als auch in der Kontrollgruppe ohne Dark Patterns, wurden die Cookies signifikant eher akzeptiert als abgelehnt.

Die Analyse des Zusammenhangs zwischen dem Einsatz von Dark Patterns und der Zustimmung zu den Cookies ergab allerdings keine signifikanten Effekte. Dies könnte auf eine zu geringe Effektstärke respektive auf eine zu schwache Manipulation oder auf eine zu geringe Stichprobengrösse zurückzuführen sein (Döring & Bortz, 2016, S. 671). Dennoch lag die Zustimmung zu den Cookies um 9.0 Prozent höher unter Einsatz von Dark Patterns im Hinweis als in der Kontrollgruppe ohne Dark Patterns. Der nicht-signifikante Zusammenhang in der vorliegenden Studie steht teilweise im Widerspruch zur Literatur, wo ein positiver Zusammenhang zwischen dem Einsatz von Dark Patterns und der Zustimmung zu Cookies nachgewiesen werden konnte (Nouwens et al., 2020, S. 9; Utz et al., 2019, S. 981).
Zu ähnlichen Resultaten wie in dieser Arbeit gelangten allerdings Grassl et al. (2021, S. 14), wo ebenfalls der Grossteil der Proband_innen die Sammlung der Cookies

akzeptierten und keine signifikanten Effekte von Dark Patterns auf die Zustimmungsentscheidung festgestellt werden konnten. In einem Folgeexperiment setzten Grassl et al. (2021, S. 20) dieselben Dark Patterns ein, um eine Ablehnung der Cookies zu erzielen, wobei signifikante Effekte festgestellt werden konnten. Die Forschenden argumentierten, dass das Ausbleiben eines Effekts von Dark Patterns auf die Zustimmung zu den Cookies damit begründet werden könnte, dass Konsument_innen darauf konditioniert wurden, dem Cookie-Hinweis zuzustimmen, da viele Webseiten dies zur Bedingung machen, um den entsprechenden Dienst nutzen zu können (Graßl et al., 2021, S. 16). Dies könnte auch in der vorliegenden Arbeit eine mögliche Begründung für das Ausbleiben der Effekte sein.

Weiter könnten auch länderspezifische Unterschiede bestehen, da in der vorliegenden Arbeit alle Proband_innen in der Schweiz ansässig waren, während die bestehenden Studien, wo Effekte nachgewiesen werden konnten, in EU-Staaten durchgeführt wurden. Von Website-Besucher_innen aus der Schweiz wird, wie in Kapitel 2.3.4 beschrieben, gemäss Stand Frühjahr 2022 nur die implizite Zustimmung zu Cookies gefordert, wodurch die Cookie-Hinweise grossteilig nur informativen Charakter haben und eine Einschränkung der Sammlung personenbezogener Daten via die Browsereinstellungen erfolgen muss (Perrot, 2019).

5.1.2 Erkennung von Dark Patterns

Die Hypothesen 2 und 3a postulierten, dass die Erkennung von Dark Patterns deren Wirkung schwächt und dass ein Zusammenhang zwischen Digitaler Kompetenz und der Fähigkeit, Dark Patterns zu erkennen, besteht. Beide Hypothesen mussten verworfen werden. In der bestehenden Forschung wurden beide Effekte ebenfalls noch nicht untersucht und nachgewiesen.

Zur Messung der Erkennung von Dark Patterns wurde auf die Skala für wahrgenommene Täuschung in der Werbung zurückgegriffen, da für die Identifikation von Dark Patterns noch keine Konstrukte erarbeitet und validiert wurden. Während die Reliabilität und Konstruktvalidität statistisch überprüft wurden, kann die Inhaltsvalidität nur theoretisch-argumentativ und gestützt durch Urteile von Fachexperten erfolgen (Döring & Bortz,

2016, S. 446). In der Prüfung auf Unterschiede zwischen der Experimental- und Kontrollgruppe hinsichtlich der gemessenen Erkennung von Dark Patterns wurden keine signifikanten Effekte nachgewiesen, was darauf hinweist, dass die Skala inhaltlich nicht valide war, da die Kontrollgruppe einen Hinweis frei von Dark Patterns beurteilte und damit signifikante Unterschiede hätten auftreten müssen. Im Unterschied zur vorliegenden Studie nutzten Di Geronimo et al. (2020) für die Messung der Erkennung von Dark Patterns die qualitative Untersuchung.

Mittels der genannten Skala wurden in der Experimentalgruppe ein Mittelwert von 3.18 und in der Kontrollgruppe ein Mittelwert von 3.01 gemessen, womit die wahrgenommene Täuschung als niedrig einzuschätzen ist. Diese Werte könnten wiederum ein Indiz dafür sein, dass die Manipulation zu schwach ausfiel. Weiter könnte auch hypothetisiert werden, dass aufgrund der weiten Verbreitung solcher Gestaltungsformen von Cookie-Zustimmungshinweisen und entsprechender Gewöhnung der Konsument_innen daran, dies nicht als Täuschung eingestuft wurde.

5.1.3 Digitale Kompetenz

Im Rahmen der Hypothesen 3a, 3b und 3c wurden der Zusammenhang zwischen Digitaler Kompetenz und der Erkennung von Dark Patterns, die Erkennung von Dark Patterns auf die Zustimmung zu den Cookies, sowie der direkte Effekt von Digitaler Kompetenz auf die Zustimmung zu den Cookies untersucht. Alle drei Hypothesen wurden verworfen.

Ebenso wurden keine signifikanten Zusammenhänge zwischen der Bildung oder des Alters, anstelle der Digitalen Kompetenz auf die genannten Variablen gemessen, was den Resultaten von Luguri und Strahilevitz (2019) und Bongard-Blanchy et al. (2021) widerspricht. In beiden genannten Studien wurden allerdings nicht spezifisch Dark Patterns im Bereich von Cookie-Zustimmungshinweisen, sondern im breiteren Website- oder Webshopping-Kontext untersucht, was möglicherweise zu unterschiedlichen Effekten geführt haben könnte.
Mit Ausnahme der Kommunikationsfertigkeit wies die Multiitem-Skala zur Messung der Digitalen Kompetenz befriedigende Cronbachs Alpha aus. Für die Auswertung wurde auf die Dimension «Kommunikationsfertigkeit» verzichtet, was die Validität der Messung

möglicherweise beeinträchtigt hatte. Weiter nannten drei Proband_innen im Feedback, dass die Beantwortung reverse-codierter Fragen schwerfiel oder besondere Aufmerksamkeit verlangte, was darauf hindeutet, dass die Komplexität der Frageformulierung allfällig zu einer Verzerrung der Resultate geführt haben könnte.

5.2 Implikationen für die Theorie

Die Resultate der Untersuchung zeigen auf, dass noch mehr Forschung zum Einsatz von Dark Patterns auf Cookie-Zustimmungshinweisen benötigt wird und die bestehende Forschung teilweise inkonsistent ist.

Die Untersuchung leistet einen Beitrag zur Erforschung der Wahrnehmung von Cookie-Zustimmungshinweisen und zur Reaktion auf dieselben in der Schweiz. Erkenntnisse spezifisch für die Schweiz sind insbesondere von Interesse, da die Einführung der Pflicht zur expliziten Zustimmung zu Cookies in Planung ist, und demnach zu erwarten ist, dass sich der Einsatz Dark Patterns in Cookie-Zustimmungshinweisen, analog zu Beobachtungen in der EU, noch weiter ausbreiten wird.

Weiter leistet die Arbeit einen Beitrag zur Validierung der Digital Literacy Skala von Rodríguez-de-Dios et al. (2016), wobei Mängel im Bereich der Messung der Kommunikationsfertigkeiten entdeckt wurden.

Die Untersuchung wirft ausserdem zusätzliche Fragen auf, welche durch weiterführende Forschung aufgegriffen werden könnten. Einige davon werden in Kapitel 5.5 aufgeführt.

5.3 Implikationen für die Praxis

Das Experiment verdeutlichte, dass die Zustimmung zu den Cookies, unabhängig vom Einsatz manipulativer Designpraktiken, sehr hoch lag. Während in dieser Arbeit keine Einblicke zu den Hintergründen für die Zustimmung geliefert wurden, können Ergebnisse vergangener Untersuchungen beigezogen werden, die aufzeigten, dass Konsument_innen ungenügend über Cookies und die Verwaltung derselben informiert sind und dass Cookie-Zustimmungshinweise unbedacht beantwortet werden (Ha et al., 2006, S. 838; Graßl et al., 2021, S. 26).

Um eine informierte und selbstbestimmte Entscheidung der Konsument_innen zu erlauben, reicht deshalb eine reine Befolgung der aktuellen regulatorischen Vorgaben nicht aus.

Sowohl Gesetzgeber als auch Unternehmen müssen Wege finden, informierte und selbstbestimmte Entscheidungen der Konsument_innen für oder gegen die Sammlung Cookies zu fördern.

5.4 Limitationen der Arbeit

Die Aussagekraft der vorliegenden Arbeit wird durch einige Faktoren limitiert, die im Folgenden erläutert werden.

5.4.1 Generalisierbarkeit

Die Generalisierbarkeit der Resultate ist eingeschränkt, da das Conceptual Model nur anhand eines konkreten Anwendungsfalls von Dark Patterns, sowie anhand einer grafischen Umsetzung überprüft wurde.

Im Vergleich der eingesetzten Manipulationen mit anderen Studien zeigte sich, dass der Cookie-Zustimmungshinweis der Experimentalgruppe fast identisch zu derjenigen von Nouwens et al. (2020) gestaltet wurde, wobei die Gestaltung des Hinweises in der Vergleichsgruppe allerdings unterschiedlich ausfiel. In der genannten Studie wurde die Alle-ablehnen-Option auf der rechten Seite platziert versus in der vorliegenden Arbeit links, was zu einer gesteigerten Interaktion mit derselben geführt haben könnte. So zeigten Eyetracking-Studien, dass die Nutzung von Websites häufig einem Muster von oben links nach unten rechts folgt, was als Gutenberg-Diagramm bezeichnet wird (Hernandez & Resnick, 2013, S. 1043). Studien zufolge sollten deshalb Call-to-Action-Buttons unten rechts platziert werden, um die Interaktion der Nutzer_innen damit zu steigern (Hernandez & Resnick, 2013, S. 1043). Um diesen Effekt auszuschliessen hätte innerhalb der Kontrollgruppe eine Randomisierung der Platzierung des Call-to-Actions erfolgen müssen.

5.4.2 Stichprobe

Es ist von einer Selbstselektions-Verzerrung der Resultate auszugehen, da die Teilnahme zum Experiment auf freiwilliger Basis beruhte (Döring & Bortz, 2016, S. 306). Während bei der Rekrutierung der Proband_innen auf Diversität hinsichtlich des Alters und der Beschäftigung geachtet wurde, sind ältere Personen schwerer erreichbar und die Befragung unter dem Titel «Digitale Kompetenz» könnte wiederum dazu geführt haben, dass Proband_innen mit sehr tiefer Digitaler Kompetenz nicht an der Befragung teilnahmen oder die Beantwortung abbrachen (Döring & Bortz, 2016, S. 363).

Weiter war das Experiment so konzipiert, dass eine Interaktion mit dem Cookie-Zustimmungshinweis erfolgen musste, bevor mit der Befragung gestartet werden konnte. Dadurch ist denkbar, dass Proband_innen mit hoher Datenschutzsensibilität die Befragung direkt abbrachen und somit nicht im Sample erfasst wurden.

5.5 Weiterführende Forschung

Auf Basis der Untersuchung lassen sich einige Fragen identifizieren, derer sich künftige Forschung annehmen sollte.

Einflussfaktoren auf die Wirkung von Dark Patterns

Die Arbeit leistete ein Versuch, mögliche Einflussfaktoren auf die Wirkung von Dark Patterns zu identifizieren. Da die Wirkung von Dark Patterns auf die unabhängige Variable nicht bestätigt werden konnte, scheiterte das Experiment diesbezüglich. Für künftige Forschung wird empfohlen, mögliche Einflussfaktoren anhand anderer, eindeutigerer Anwendungsfelder von Dark Patterns als Cookie-Zustimmungshinweise zu untersuchen, um signifikante Ergebnisse zu erzielen.

Dark Patterns auf Cookie-Zustimmungshinweisen

Während im Experiment kein Zusammenhang zwischen dem Einsatz von Dark Patterns und der Zustimmung zur Sammlung von Cookies festgestellt werden konnte, empfiehlt es sich die Untersuchung im Rahmen eines Feldexperiments, unter natürlichen Bedingungen mit einem grösseren Sample, zu wiederholen, um mögliche Einflüsse des künstlich konstruierten Settings auszuschliessen.

Weiter sollten auch andere Untersuchungsmethoden wie der Mixed-Method-Ansatz oder Lautes Denken geprüft werden, um Einblick in die Hintergründe für die Entscheidung der Konsument_innen für oder gegen Cookies zu erhalten.

Digitale Kompetenz

Die Digital Literacy Skala von Rodríguez-de-Dios et al. (2016) wies Schwächen in der Messung der Kommunikationsfertigkeit auf. Weitergehende Forschung sollte sich der Überarbeitung und erneuten Validierung der Skala widmen.

6 Literaturverzeichnis

Backhaus, K., Erichson, B., Plinke, W., & Weiber, R. (2016). *Multivariate Analysemethoden*. Springer Berlin Heidelberg. https://doi.org/10.1007/978-3-662-46076-4

Baker, S. M., Gentry, J. W., & Rittenburg, T. L. (2005). Building Understanding of the Domain of Consumer Vulnerability. *Journal of Macromarketing*, *25*(2), 128-139. https://doi.org/10.1177/0276146705280622

Baroni, L. A., Puska, A. A., de Castro Salgado, L. C., & Pereira, R. (2021). Dark Patterns: Towards a Socio-technical Approach. *Proceedings of the XX Brazilian Symposium on Human Factors in Computing Systems*, 1-7. https://doi.org/10.1145/3472301.3484336

Baur, N., & Blasius, J. (2014). Methoden der empirischen Sozialforschung. In N. Baur & J. Blasius (Hrsg.), *Handbuch Methoden der empirischen Sozialforschung* (S. 41-64). Springer Fachmedien Wiesbaden. https://doi.org/10.1007/978-3-531-18939-0

Beck, H. (2014). *Behavioral Economics*. Springer Fachmedien Wiesbaden. https://doi.org/10.1007/978-3-658-03367-5

Bentler, P. M. (1990). Comparative fit indexes in structural models. *Psychological Bulletin*, *107*(2), 238. https://doi.org/10.1037/0033-2909.107.2.238

Berekoven, L., Eckert, W., & Ellenrieder, P. (2009). *Marktforschung: Methodische Grundlagen und praktische Anwendung* (12. Auflage). Gabler.

Bogenstahl, C. (2019). *Dark Patterns – Mechanismen (be)trügerischen Internetdesigns*. Büro für Technikfolgen-Abschätzung beim Deutschen Bundestag.

Bongard-Blanchy, K., Rossi, A., Rivas, S., Doublet, S., Koenig, V., & Lenzini, G. (2021). ”I am Definitely Manipulated, Even When I am Aware of it. It’s Ridiculous!”—Dark Patterns from the End-User Perspective. *Designing Interactive Systems Conference 2021*, 763-776. https://doi.org/10.1145/3461778.3462086

Bortz, J., & Döring, N. (2006). *Forschungsmethoden und Evaluation: Für Human- und Sozialwissenschaftler* (4.Auflage). Springer.

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*, 237-254. https://doi.org/10.1515/popets-2016-0038

Brignull, H. (2010a). *Misdirection—A type of deceptive design*. https://www.deceptive.design/types/misdirection

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

Brignull, H. (2010c). *What is deceptive design?* https://www.deceptive.design/

Brzezicka, J., & Wisniewski, R. (2014). Homo Oeconomicus and Behavioral Economics. *Contemporary Economics*, *8*(4), 353-364. https://doi.org/10.5709/ce.1897-9254.150

Bundesamt für Statistik. (2021). *Ungleiche Verteilung digitaler Kompetenzen bei Internetnutzerinnen und -nutzern in der Schweiz*. https://www.swissstats.bfs.admin.ch/collection/ch.admin.bfs.swissstat.de.issue211620901900/article/issue211620901900-01

Bundesamt für Statistik. (2022a). *Digitale Kompetenzen*. https://www.bfs.admin.ch/bfs/de/home/statistiken/kultur-medien-informationsgesellschaft-sport/informationsgesellschaft/gesamtindikatoren/haushalte-bevoelkerung/digitalekompetenzen.html

Bundesamt für Statistik. (2022b). *SAKE – Schweizerische Arbeitskräfteerhebung. Variablenliste und Struktur des SAKE-Fragebogens 2021*. https://www.bfs.admin.ch/bfs/de/home/statistiken/arbeit-erwerb/erhebungen/sake.assetdetail.20565828.html

Burr, C., Cristianini, N., & Ladyman, J. (2018). An Analysis of the Interaction Between Intelligent Software Agents and Human Users. *Minds and Machines*, *28*(4), 735-774. https://doi.org/10.1007/s11023-018-9479-0

Calo, M. R. (2014). Digital Market Manipulation. *The George Washington Law Review*, *82*(995), 995-1051.

Chivukula, S. S., Watkins, C., McKay, L., & Gray, C. M. (2019). «Nothing Comes Before Profit»: Asshole Design In the Wild. *Conference on Human Factors in Computing Systems*, 1-6. https://doi.org/10.1145/3290607.3312863

Citizens Advice. (2016). *Locked in. Consumer issues with subscription traps*. https://www.citizensadvice.org.uk/Global/CitizensAdvice/Consumer%20publications/Finaldraft-Lockedinconsumerissueswithsubscriptiontraps%20(1).pdf

Competition & Markets Authority. (2019). *Consumer vulnerability: Challenges and potential solutions* (S. 41). https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/782542/CMA-Vulnerable_People_Accessible.pdf

Cookiebot. (2021). *Cookie-Texte und Cookie Hinweise im Zeitalter des Privacy Paradox*. https://www.cookiebot.com/de/cookie-texte/

Degeling, M., Utz, C., Lentzsch, C., Hosseini, H., Schaub, F., & Holz, T. (2019). We Value Your Privacy ... Now Take Some Cookies: Measuring the GDPR's Impact on Web Privacy. *Proceedings 2019 Network and Distributed System Security Symposium*. Network and Distributed System Security Symposium. https://doi.org/10.14722/ndss.2019.23378

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

DiMaggio, P., & Hargittai, E. (2001). *From the «Digital Divide» to «Digital Inequality»: Studying Internet Use as Penetration Increases* (Working Paper Nr. 15). Center for Arts and Cultural Policy Studies.

Döring, N., & Bortz, J. (2016). *Forschungsmethoden und Evaluation in den Sozial- und Humanwissenschaften*. Springer Berlin Heidelberg. https://doi.org/10.1007/978-3-642-41089-5

Eifler, S. (2014). Experiment. In N. Baur & J. Blasius (Hrsg.), *Handbuch Methoden der empirischen Sozialforschung* (S. 195-210). Springer Fachmedien Wiesbaden. https://doi.org/10.1007/978-3-531-18939-0

Eshet-Alkalai, Y. (2004). Digital Literacy: A Conceptual Framework for Survival Skills in the Digital era. *Journal of Educational Multimedia and Hypermedia*, *13*(1), 93-106.

Fabrigar, L. R., Wegener, D. T., MacCallum, R. C., & Strahan, E. J. (1999). Evaluating the use of exploratory factor analysis in psychological research. *Psychological Methods*, *4*(3), 272. https://doi.org/10.1037/1082-989X.4.3.272

George, D., & Mallery. (2003). SPSS for Windows step by step: A simple guide and reference, 18.0 update. In *SPSS for Windows step by step a simple guide and reference, 18.0 update* (4.Auflage). Allyn & Bacon.

Graßl, P., Schraffenberger, H., Borgesius, F. Z., & Buijzen, M. (2021). Dark and bright patterns in cookie consent requests. *Journal of Digital Social Research*, *3*(1), 1-38.

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

Grazioli, S., & Jarvenpaa, S. L. (2000). Perils of Internet fraud: An empirical investigation of deception and trust with experienced Internet consumers. *IEEE Transactions on Systems, Man, and Cybernetics - Part A: Systems and Humans*, *30*(4), 395-410. https://doi.org/10.1109/3468.852434

Gunawan, J., Pradeep, A., Choffnes, D., Hartzog, W., & Wilson, C. (2021). A Comparative Study of Dark Patterns Across Web and Mobile Modalities. *Proceedings of the ACM on Human-Computer Interaction*, *5*, 1-29. https://doi.org/10.1145/3479521

Ha, V., Inkpen, K., Al Shaar, F., & Hdeib, L. (2006). An examination of user perception and misconception of internet cookies. *CHI '06 Extended Abstracts on Human Factors in Computing Systems*, 833-838. https://doi.org/10.1145/1125451.1125615

Häder, M. (2019). *Empirische Sozialforschung: Eine Einführung*. Springer Fachmedien Wiesbaden. https://doi.org/10.1007/978-3-658-26986-9

Hargreaves Heap, S. P. (2013). What is the meaning of behavioural economics? *Cambridge Journal of Economics*, *37*(5), 985-1000. https://doi.org/10.1093/cje/bes090

Häubl, G., & Murray, K. B. (2005). «Double Agents»: Assessing the Role of Electronic Product Recommendation Systems. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.964191

Helsper, E. J. (2008). *Digital inclusion: An analysis of social disadvantage and the information society*. Department for Communities and Local Government. http://www.communities.gov.uk/documents/communities/pdf/digitalinclusionanalysis

Hermstrüwer, Y. (2017). *Contracting Around Privacy: The (Behavioral) Law and Economics of Consent and Big Data* (S. 9-26). JIPITEC.

Hernandez, A., & Resnick, M. L. (2013). Placement of Call to Action Buttons for Higher Website Conversion and Acquisition: An Eye Tracking Study. *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*, *57*, 1042-1046. https://doi.org/10.1177/1541931213571232

Hidalgo, A., Gabaly, S., Morales-Alonso, G., & Urueña, A. (2020). The digital divide in light of sustainable development: An approach through advanced machine learning techniques. *Technological Forecasting and Social Change*, *150*, 119754. https://doi.org/10.1016/j.techfore.2019.119754

Hill, R. P., & Sharma, E. (2020). Consumer Vulnerability. *Journal of Consumer Psychology*, *30*(3), 551-570. https://doi.org/10.1002/jcpy.1161

Himme, A. (2009). Gütekriterien der Messung: Reliabilität, Validität und Generalisierbarkeit. In S. Albers, D. Klapper, U. Konradt, A. Walter, & J. Wolf (Hrsg.), *Methodik der empirischen Forschung* (S. 485-500). Gabler Verlag. https://doi.org/10.1007/978-3-322-96406-9

Hu, L., & Bentler, P. M. (1999). Cutoff criteria for fit indexes in covariance structure analysis: Conventional criteria versus new alternatives. *Structural Equation Modeling: A Multidisciplinary Journal*, *6*(1), 1-55. https://doi.org/10.1080/10705519909540118

Huber, F., Meyer, F., & Lenzen, M. (2014). *Grundlagen der Varianzanalyse*. Springer Fachmedien Wiesbaden. https://doi.org/10.1007/978-3-658-05666-7

Hussy, W., Schreier, M., & Echterhoff, G. (2010). *Forschungsmethoden in Psychologie und Sozialwissenschaften: Für Bachelor*. Springer.

Jacobs, G. E., Castek, J., Pizzolato, A., Reder, S., & Pendell, K. (2014). Production and Consumption. *Journal of Adolescent & Adult Literacy*, *57*(8), 624-627. https://doi.org/10.1002/jaal.293

Johnson, E. J., Shu, S. B., Dellaert, B. G. C., Fox, C., Goldstein, D. G., Häubl, G., Larrick, R. P., Payne, J. W., Peters, E., Schkade, D., Wansink, B., & Weber, E. U. (2012). Beyond nudges: Tools of a choice architecture. *Marketing Letters*, *23*(2), 487-504. https://doi.org/10.1007/s11002-012-9186-1

Kahneman, D. (2003). Maps of Bounded Rationality: Psychology for Behavioral Economics. *American Economic Review*, *93*(5), 1449-1475. https://doi.org/10.1257/000282803322655392

Kahneman, D. (2011). *Thinking, fast and slow*. Farrar, Straus and Giroux.

Koltay, T. (2011). The media and the literacies: Media literacy, information literacy, digital literacy. *Media, Culture & Society*, *33*(2), 211-221. https://doi.org/10.1177/0163443710393382

Konsumentverket. (2021). *Barriers to a well-functioning digital market. Effects of visual design and information disclosures on consumer detriment* (Underlagsrapport 2021 Nr. 1; S. 72).

Kucuk, S. U. (2016). Consumerism in the Digital Age. *Journal of Consumer Affairs*, *50*(3), 515-538. https://doi.org/10.1111/joca.12101

Kuhlemeier, H., & Hemker, B. (2007). The impact of computer use at home on students' Internet skills. *Computers & Education*, *49*(2), 460-480. https://doi.org/10.1016/j.compedu.2005.10.004

Kuss, A., Wildner, R., & Kreis, H. (2014). *Marktforschung*. Springer Fachmedien Wiesbaden. https://doi.org/10.1007/978-3-658-01864-1

Lacey, C., & Caudwell, C. (2019). Cuteness as a 'Dark Pattern' in Home Robots. *2019 14th ACM/IEEE International Conference on Human-Robot Interaction (HRI)*, 374-381. https://doi.org/10.1109/HRI.2019.8673274

Lades, L. K., & Delaney, L. (2022). Nudge FORGOOD. *Behavioural Public Policy*, *6*(1), 75-94. https://doi.org/10.1017/bpp.2019.53

Lewis, C. (2014). Irresistible apps: Motivational design patterns for apps, games, and web-based communities. In *Irresistible apps motivational design patterns for apps, games, and web-based communities*. Apress.

Luguri, J., & Strahilevitz, L. J. (2019). Shining a Light on Dark Patterns. *Journal of Legal Analysis*, *13*(43). https://dx.doi.org/10.2139/ssrn.3431205

Lukoff, K., Hiniker, A., Gray, C. M., Mathur, A., & Chivukula, S. S. (2021). What Can CHI Do About Dark Patterns? *Extended Abstracts of the 2021 CHI Conference on Human Factors in Computing Systems*, 1-6. https://doi.org/10.1145/3411763.3441360

Lythreatis, S., Singh, S. K., & El-Kassar, A.-N. (2022). The digital divide: A review and future research agenda. *Technological Forecasting and Social Change*, *175*, 121359. https://doi.org/10.1016/j.techfore.2021.121359

Maddox, R. N. (1982). The structure of consumers' satisfaction: Cross-product comparisons. *‚Journal of the Academy of Marketing Science*, *10*(1), 37-53.

Maier, M., & Harr, R. (2020). Dark Design Patterns: An End-User Perspective. *Human Technology*, *16*(2), 170-199. https://doi.org/10.17011/ht/urn.202008245641

Marchiori, D. R., Adriaanse, M. A., & De Ridder, D. T. D. (2017). Unresolved questions in nudging research: Putting the psychology back in nudging. *Social and Personality Psychology Compass*, *11*(1), e12297. https://doi.org/10.1111/spc3.12297

Martin, A. (2005). DigEuLit – a European Framework for Digital Literacy: A Progress Report. *Journal of eLiteracy*, *2*.

Martin, A., & Grudziecki, J. (2006). DigEuLit: Concepts and Tools for Digital Literacy Development. *Innovation in Teaching and Learning in Information and Computer Sciences*, *5*(4), 249-267. https://doi.org/10.11120/ital.2006.05040249

Mathur, A. (2021). Identifying and Measuring Manipulative User Interfaces at Scale on the Web. *Extended Abstracts of the 2021 CHI Conference on Human Factors in Computing Systems*, 1-5. https://doi.org/10.1145/3411763.3457782

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

Mathur, A., Mayer, J., & Kshirsagar, M. (2021). What Makes a Dark Pattern... Dark? Design Attributes, Normative Considerations, and Measurement Methods. *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*, 1-18. https://doi.org/10.1145/3411764.3445610

Matte, C., Bielova, N., & Santos, C. (2020). Do Cookie Banners Respect my Choice? : Measuring Legal Compliance of Banners from IAB Europe's Transparency and Consent Framework. *2020 IEEE Symposium on Security and Privacy (SP)*, 791-809. https://doi.org/10.1109/SP40000.2020.00076

Mellet, K., & Beauvisage, T. (2020). Cookie monsters. Anatomy of a digital market infrastructure. *Consumption Markets & Culture*, *23*(2), 110-129. https://doi.org/10.1080/10253866.2019.1661246

Mirsch, T., Lehrer, C., & Jung, R. (2017). Digital Nudging: Altering User Behavior in Digital Environments. *Proceedings Der 13. Internationalen Tagung Wirtschaftsinformatik (WI 2017)*, 634-648.

Moser, C., Schoenebeck, S. Y., & Resnick, P. (2019). Impulse Buying: Design Practices and Consumer Needs. *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*, 1-15. https://doi.org/10.1145/3290605.3300472

Murray, K. B., Liang, J., & Häubl, G. (2010). ACT 2.0: The next generation of assistive consumer technology research. *Internet Research*, *20*(3), 232-254. https://doi.org/10.1108/10662241011050696

Nouwens, M., Liccardi, I., Veale, M., Karger, D., & Kagal, L. (2020). Dark Patterns after the GDPR: Scraping Consent Pop-ups and Demonstrating their Influence. *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*, 1-13. https://doi.org/10.1145/3313831.3376321

Office for Official Publications of the European Communities. (2003). *eLearning: Better eLearning for Europe Directorate- General for Education and Culture.*

Oppenheimer, D. M., Meyvis, T., & Davidenko, N. (2009). Instructional manipulation checks: Detecting satisficing to increase statistical power. *Journal of Experimental Social Psychology*, *45*(4), 867-872.

Perrot, C. (2019). *Rechtskonforme Cookie-Hinweise*. Swiss Infosec. https://www.infosec.ch/blog/rechtskonforme-cookie-hinweise

Peterson, R. A. (1994). A Meta-Analysis of Cronbach's Coefficient Alpha. *Journal of Consumer Research*, *21*(2), 381-391.

Reddy, P., Sharma, B., & Chaudhary, K. (2020). Digital Literacy: A Review of Literature. *International Journal of Technoethics*, *11*(2), 65-94. https://doi.org/10.4018/IJT.20200701.oa1

Reisch, L. A. (2020). *Nudging hell und dunkel: Regeln für digitales Nudging* (S. 87-91). Wirtschaftsdienst. http://link.springer.com/10.1007/s10273-020-2573-y

Riggins, F., & Dewan, S. (2005). The Digital Divide: Current and Future Research Directions. *Journal of the Association for Information Systems*, *6*(12), 298-337. https://doi.org/10.17705/1jais.00074

Rodríguez-de-Dios, I., & Igartua, J.-J. (2016). Skills of Digital Literacy to Address the Risks of Interactive Communication: *Journal of Information Technology Research*, *9*(1), 54-64. https://doi.org/10.4018/JITR.2016010104

Rodríguez-de-Dios, I., van Oosten, J. M. F., & Igartua, J.-J. (2018). A study of the relationship between parental mediation and adolescents' digital skills, online risks and online opportunities. *Computers in Human Behavior*, *82*, 186-198. https://doi.org/10.1016/j.chb.2018.01.012

Sanchez-Rola, I., Dell'Amico, M., Kotzias, P., Balzarotti, D., Bilge, L., Vervier, P.-A., & Santos, I. (2019). Can I Opt Out Yet?: GDPR and the Global Illusion of Cookie Control. *Proceedings of the 2019 ACM Asia Conference on Computer and Communications Security*, 340-351. https://doi.org/10.1145/3321705.3329806

Schmidt, A. T. (2017). The Power to Nudge. *American Political Science Review*, *111*(2), 404-417. https://doi.org/10.1017/S0003055417000028

Schweizerische Eidgenossenschaft. (1997). *Fernmeldegesetz (FMG)*. https://www.fedlex.admin.ch/eli/cc/1997/2187_2187_2187/de

Schweizerische Eidgenossenschaft. (2022). *Stärkung des Datenschutzes*. Bundesamt für Justiz BJ. https://www.bj.admin.ch/bj/de/home/staat/gesetzgebung/datenschutzstaerkung.html

Simon, H. A. (1955). A Behavioral Model of Rational Choice. *The Quarterly Journal of Economics*, *69*(1), 239-258. https://doi.org/10.2307/1884852

Sin, R., Harris, T., Nilsson, S., & Beck, T. (2022). Dark patterns in online shopping: Do they work and can nudges help mitigate impulse buying? *Behavioural Public Policy*, 1-27. https://doi.org/10.1017/bpp.2022.11

Smith, Dinev, & Xu. (2011). Information Privacy Research: An Interdisciplinary Review. *MIS Quarterly*, *35*(4), 989. https://doi.org/10.2307/41409970

Soe, T. H., Nordberg, O. E., Guribye, F., & Slavkovik, M. (2020). Circumvention by design—Dark patterns in cookie consent for online news outlets. *Proceedings of the 11th Nordic Conference on Human-Computer Interaction: Shaping Experiences, Shaping Society*, 1-12. https://doi.org/10.1145/3419249.3420132

Sonck, N., & de Haan, J. (2013). How The Internet Skills Of European 11- To 16-Year-Olds Mediate Between Online Risk And Harm. *Journal of Children and Media*, *7*(1), 79-95. https://doi.org/10.1080/17482798.2012.739783

Stanovich, K. E., & West, R. F. (2000). Individual differences in reasoning: Implications for the rationality debate? *Behavioral and Brain Sciences*, *23*(5), 645-665. https://doi.org/10.1017/S0140525X00003435

Sunstein, C. R. (2020). Sludge Audits. *Behavioural Public Policy*, 1-20. https://doi.org/10.1017/bpp.2019.32

Sury, U. (2017). Revision Datenschutz in der Schweiz. *Informatik-Spektrum*, *40*(2), 221-226. https://doi.org/10.1007/s00287-017-1022-9

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

Thaler, R. H., & Sunstein, C. R. (2009). *Nudge: Improving decisions about health, wealth, and happiness*. Penguin Books.

Tondeur, J., Aesaert, K., Pynoo, B., Braak, J., Fraeyman, N., & Erstad, O. (2017). Developing a validated instrument to measure preservice teachers' ICT competencies: Meeting the demands of the 21st century. *British Journal of Educational Technology*, *48*(2), 462-472. https://doi.org/10.1111/bjet.12380

Tornero Pérez, J. M. (2004). *Promoting Digital Literacy*.

Treiblmaier, H. (2010). Datenqualität und Validität bei Online-Befragungen. *der markt*, *50*, 3-18. https://doi.org/10.1007/s12642-010-0030-y

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

Universität Zürich. (2022a). *Einfache lineare Regression*. Universität Zürich. http://www.methodenberatung.uzh.ch/de/datenanalyse_spss/zusammenhaenge/ereg.html

Universität Zürich. (2022b). *Mann-Whitney-U-Test*. Universität Zürich. http://www.methodenberatung.uzh.ch/de/datenanalyse_spss/unterschiede/zentral/mann.html

Universität Zürich. (2022c). *Pearson Chi-Quadrat-Test (Kontingenzanalyse)*. Universität Zürich. http://www.methodenberatung.uzh.ch/de/datenanalyse_spss/zusammenhaenge/pearsonzush.html

Universität Zürich. (2022d). *T-Test für unabhängige Stichproben*. Universität Zürich. http://www.methodenberatung.uzh.ch/de/datenanalyse_spss/unterschiede/zentral/ttestunabh.html

Utz, C., Degeling, M., Fahl, S., Schaub, F., & Holz, T. (2019). (Un)informed Consent: Studying GDPR Consent Notices in the Field. *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security*, 973-990. https://doi.org/10.1145/3319535.3354212

van Deursen, A. J. A. M., van Dijk, J. A. G. M., & Peters, O. (2012). Proposing a Survey Instrument for Measuring Operational, Formal, Information, and Strategic Internet Skills. *International Journal of Human-Computer Interaction*, *28*(12), 827-837. https://doi.org/10.1080/10447318.2012.670086

van Dijk, J. (2005). *The Deepening Divide: Inequality in the Information Society*. SAGE Publications, Inc. https://doi.org/10.4135/9781452229812

Wei, K.-K., Teo, H.-H., Chan, H. C., & Tan, B. C. Y. (2011). Conceptualizing and Testing a Social Cognitive Model of the Digital Divide. *Information Systems Research*, *22*(1), 170-187.

Weichbold, M. (2014). Pretest. In N. Baur & J. Blasius (Hrsg.), *Handbuch Methoden der empirischen Sozialforschung* (S. 299-304). Springer Fachmedien Wiesbaden. https://doi.org/10.1007/978-3-531-18939-0

Weinmann, M., Schneider, C., & vom Brocke, J. (2016). Digital Nudging. *Business & Information Systems Engineering*, *58*(6), 433-436. https://doi.org/10.1007/s12599-016-0453-1

Wilson, M., Scalise, K., & Gochyyev, P. (2015). Rethinking ICT literacy: From computer skills to social network settings. *Thinking Skills and Creativity*, *18*, 65-80. https://doi.org/10.1016/j.tsc.2015.05.001

Zagal, J. P., Björk, S., & Lewis, C. (2013). Dark Patterns in the Design of Games. *Presented at the Foundations of Digital Games 2013*, 1-8.

Zalando. (o. J.). Zalando. www.zalando.ch

7 Anhang

7.1 Anhang A: Finaler Fragebogen

Nr	Variable	Skalenart	Text
-	-	Introtext	Liebe/r Teilnehmer/in Vielen Dank für Ihre Teilnahme an der vorliegenden Befragung zum Thema Digitale Kompetenz im Rahmen meiner Masterarbeit an der Zürcher Hochschule für Angewandte Wissenschaften. Die Befragung dauert ungefähr 7 Minuten. Die Auswertung der Befragung erfolgt anonym. Die Daten werden ausschliesslich im Rahmen dieser Forschungsarbeit verwendet und anschliessend gelöscht. Unter sämtlichen Teilnehmenden werden drei mal CHF 50 verlost. Für allfällige Fragen sowie Feedback stehe ich gerne via [redacted] zur Verfügung. Vielen Dank für Ihre Unterstützung. Beste Grüsse, Larissa Mörgeli
			Teil 1: Abfrage Digitale Kompetenz

1*	ts_1	7-Punkt Likert-Skala (1 Stimme überhaupt nicht zu, 7 Stimme voll zu)	**Ich weiss, wie ich eine Webseite, die mir gefällt, mit einem Lesezeichen versehe (oder als Favorit speichere), damit ich sie mir später ansehen kann.** Bitte bewerten Sie anhand der Skala, inwiefern die jeweilige Aussage auf Sie zutrifft. Die Skala reicht von “Stimme überhaupt nicht zu” bis “Stimme voll zu”.
2*	ts_2	7-Punkt Likert-Skala (1 Stimme überhaupt nicht zu, 7 Stimme voll zu)	**Ich weiss immer, wie ich ein Foto, das ich online gefunden habe, herunterladen/speichern kann.** Bitte bewerten Sie anhand der Skala, inwiefern die jeweilige Aussage auf Sie zutrifft. Die Skala reicht von “Stimme überhaupt nicht zu” bis “Stimme voll zu”.
3*	ts_3	7-Punkt Likert-Skala (1 Stimme überhaupt nicht zu, 7 Stimme voll zu)	**Ich weiss, wie ich Informationen (bspw. Zeitungsartikel), die ich online gefunden habe, herunterladen kann.** Bitte bewerten Sie anhand der Skala, inwiefern die jeweilige Aussage auf Sie zutrifft. Die Skala reicht von “Stimme überhaupt nicht zu” bis “Stimme voll zu”.

4*	ts_4	7-Punkt Likert-Skala (1 Stimme überhaupt nicht zu, 7 Stimme voll zu)	**Ich weiss immer, wie ich eine Verbindung zu einem WLAN-Netzwerk herstellen kann, unabhängig vom Gerät oder wo ich mich befinde.** Bitte bewerten Sie anhand der Skala, inwiefern die jeweilige Aussage auf Sie zutrifft. Die Skala reicht von “Stimme überhaupt nicht zu” bis “Stimme voll zu”.
5*	ts_5	7-Punkt Likert-Skala (1 Stimme überhaupt nicht zu, 7 Stimme voll zu)	**Ich weiss, wie man Tastenkombinationen verwendet (z. B. CTRL + C, Strg + C oder cmd + C für kopieren).** Bitte bewerten Sie anhand der Skala, inwiefern die jeweilige Aussage auf Sie zutrifft. Die Skala reicht von “Stimme überhaupt nicht zu” bis “Stimme voll zu”.
6*	ts_6 (reverse)	7-Punkt Likert-Skala (1 Stimme überhaupt nicht zu, 7 Stimme voll zu)	**Ich lade nicht gerne Apps für Smartphones herunter, da es mir schwer fällt, ihre Bedienung zu erlernen.** Bitte bewerten Sie anhand der Skala, inwiefern die jeweilige Aussage auf Sie zutrifft. Die Skala reicht von “Stimme überhaupt nicht zu” bis “Stimme voll zu”.

7*	ts_7 (reverse)	7-Punkt Likert-Skala (1 Stimme überhaupt nicht zu, 7 Stimme voll zu)	**Wenn ich neue Programme auf meinem Computer installieren möchte, dann bitte ich jemanden, dies für mich zu tun, weil ich nicht weiss, wie es geht.** Bitte bewerten Sie anhand der Skala, inwiefern die jeweilige Aussage auf Sie zutrifft. Die Skala reicht von “Stimme überhaupt nicht zu” bis “Stimme voll zu”.
8*	pss_1	7-Punkt Likert-Skala (1 Stimme überhaupt nicht zu, 7 Stimme voll zu)	**Ich weiss, wie ich die Funktion zur Anzeige meiner geografischen Position deaktivieren kann (z. B. Facebook, Apps).** Bitte bewerten Sie anhand der Skala, inwiefern die jeweilige Aussage auf Sie zutrifft. Die Skala reicht von “Stimme überhaupt nicht zu” bis “Stimme voll zu”.
9*	pss_2	7-Punkt Likert-Skala (1 Stimme überhaupt nicht zu, 7 Stimme voll zu)	**Ich weiss, wann ich rechtlich gesehen Bilder und Videos von anderen Menschen online stellen darf.** Bitte bewerten Sie anhand der Skala, inwiefern die jeweilige Aussage auf Sie zutrifft. Die Skala reicht von “Stimme überhaupt nicht zu” bis “Stimme voll zu”.
10*	pss_3	7-Punkt Likert-Skala (1 Stimme	**Ich weiss, wie man die «Missbrauch melden» Buttons auf sozialen Medien**

		überhaupt nicht zu, 7 Stimme voll zu)	**verwendet (z. B. wenn jemand mein Foto ohne meine Erlaubnis verwendet).** Bitte bewerten Sie anhand der Skala, inwiefern die jeweilige Aussage auf Sie zutrifft. Die Skala reicht von “Stimme überhaupt nicht zu” bis “Stimme voll zu”.
11*	pss_4	7-Punkt Likert-Skala (1 Stimme überhaupt nicht zu, 7 Stimme voll zu)	**Ich weiss, wie ich die Privatsphäre-Einstellungen auf den sozialen Medien anpassen kann, um festzulegen, was andere von mir sehen können (Freunde von Freunden, nur Freunde, nur ich).** Bitte bewerten Sie anhand der Skala, inwiefern die jeweilige Aussage auf Sie zutrifft. Die Skala reicht von “Stimme überhaupt nicht zu” bis “Stimme voll zu”.
12*	cs_1	7-Punkt Likert-Skala (1 Stimme überhaupt nicht zu, 7 Stimme voll zu)	**Ich weiss, wie man verschiedene Quellen vergleichen kann, um zu entscheiden, ob die Informationen wahr sind.** Bitte bewerten Sie anhand der Skala, inwiefern die jeweilige Aussage auf Sie zutrifft. Die Skala reicht von “Stimme überhaupt nicht zu” bis “Stimme voll zu”.

13*	cs_2	7-Punkt Likert-Skala (1 Stimme überhaupt nicht zu, 7 Stimme voll zu)	**Ich weiss, wie ich feststellen kann, ob die Informationen, die ich online finde, zuverlässig sind.** Bitte bewerten Sie anhand der Skala, inwiefern die jeweilige Aussage auf Sie zutrifft. Die Skala reicht von "Stimme überhaupt nicht zu" bis "Stimme voll zu".
14*	cs_3	7-Punkt Likert-Skala (1 Stimme überhaupt nicht zu, 7 Stimme voll zu)	**Ich weiss, wie ich den Autor der Informationen identifizieren und ihre Zuverlässigkeit bewerten kann.** Bitte bewerten Sie anhand der Skala, inwiefern die jeweilige Aussage auf Sie zutrifft. Die Skala reicht von "Stimme überhaupt nicht zu" bis "Stimme voll zu".
15*	cs_4	7-Punkt Likert-Skala (1 Stimme überhaupt nicht zu, 7 Stimme voll zu)	**Ich weiss, wie ich verschiedene Apps vergleichen kann, um auszuwählen, welche die zuverlässigste und sicherste ist.** Bitte bewerten Sie anhand der Skala, inwiefern die jeweilige Aussage auf Sie zutrifft. Die Skala reicht von "Stimme überhaupt nicht zu" bis "Stimme voll zu".
16*	cs_5	7-Punkt Likert-Skala (1 Stimme überhaupt nicht zu, 7 Stimme voll zu)	**Wenn ich jemanden online kennenlerne, weiss ich, wie ich überprüfen kann, ob sein Profil echt ist.**

			Bitte bewerten Sie anhand der Skala, inwiefern die jeweilige Aussage auf Sie zutrifft. Die Skala reicht von “Stimme überhaupt nicht zu” bis “Stimme voll zu”.
17*	dss_1	7-Punkt Likert-Skala (1 Stimme überhaupt nicht zu, 7 Stimme voll zu)	**Ich verwende Software um Viren zu erkennen und entfernen.** Bitte bewerten Sie anhand der Skala, inwiefern die jeweilige Aussage auf Sie zutrifft. Die Skala reicht von “Stimme überhaupt nicht zu” bis “Stimme voll zu”.
18*	dss_2	7-Punkt Likert-Skala (1 Stimme überhaupt nicht zu, 7 Stimme voll zu)	**Ich weiss, wie ich einen Virus in meinem digitalen Gerät erkennen kann.** Bitte bewerten Sie anhand der Skala, inwiefern die jeweilige Aussage auf Sie zutrifft. Die Skala reicht von “Stimme überhaupt nicht zu” bis “Stimme voll zu”.
19*	dss_3	7-Punkt Likert-Skala (1 Stimme überhaupt nicht zu, 7 Stimme voll zu)	**Ich weiss, wie man unerwünschte oder Junk-Mails/Spam blockiert.** Bitte bewerten Sie anhand der Skala, inwiefern die jeweilige Aussage auf Sie zutrifft. Die Skala reicht von “Stimme überhaupt nicht zu” bis “Stimme voll zu”.

20*	dss_4	7-Punkt Likert-Skala (1 Stimme überhaupt nicht zu, 7 Stimme voll zu)	**Wenn etwas nicht funktioniert, während ich ein Gerät (Computer, Smartphone usw.) benutze, weiss ich in der Regel, was es ist und wie ich das Problem beheben kann.** Bitte bewerten Sie anhand der Skala, inwiefern die jeweilige Aussage auf Sie zutrifft. Die Skala reicht von "Stimme überhaupt nicht zu" bis "Stimme voll zu".
21*	is_1 (reverse)	7-Punkt Likert-Skala (1 Stimme überhaupt nicht zu, 7 Stimme voll zu)	**Es fällt mir schwer zu entscheiden, welches die besten Suchbegriffe für die Online-Suche sind.** Bitte bewerten Sie anhand der Skala, inwiefern die jeweilige Aussage auf Sie zutrifft. Die Skala reicht von "Stimme überhaupt nicht zu" bis "Stimme voll zu".
22*	is_2 (reverse)	7-Punkt Likert-Skala (1 Stimme überhaupt nicht zu, 7 Stimme voll zu)	**Ich finde die Art und Weise, wie viele Websites gestaltet sind, verwirrend.** Bitte bewerten Sie anhand der Skala, inwiefern die jeweilige Aussage auf Sie zutrifft. Die Skala reicht von "Stimme überhaupt nicht zu" bis "Stimme voll zu".
23*	is_3 (reverse)	7-Punkt Likert-Skala (1 Stimme überhaupt nicht zu, 7 Stimme voll zu)	**Manchmal fällt es mir schwer zu bestimmen, wie nützlich die Informationen, die ich online**

			gefunden habe, für meine Zwecke sind. Bitte bewerten Sie anhand der Skala, inwiefern die jeweilige Aussage auf Sie zutrifft. Die Skala reicht von "Stimme überhaupt nicht zu" bis "Stimme voll zu".
24*	is_4 (reverse)	7-Punkt Likert-Skala (1 Stimme überhaupt nicht zu, 7 Stimme voll zu)	**Ich werde schnell müde, wenn ich online nach Informationen suche.** Bitte bewerten Sie anhand der Skala, inwiefern die jeweilige Aussage auf Sie zutrifft. Die Skala reicht von "Stimme überhaupt nicht zu" bis "Stimme voll zu".
25*	is_5 (reverse)	7-Punkt Likert-Skala (1 Stimme überhaupt nicht zu, 7 Stimme voll zu)	**Manchmal lande ich auf Websites, ohne zu wissen, wie ich dort hingekommen bin.** Bitte bewerten Sie anhand der Skala, inwiefern die jeweilige Aussage auf Sie zutrifft. Die Skala reicht von "Stimme überhaupt nicht zu" bis "Stimme voll zu".
26*	coms_1	7-Punkt Likert-Skala (1 Stimme überhaupt nicht zu, 7 Stimme voll zu)	**Je nachdem, mit wem ich kommunizieren möchte, ist es besser, eine bestimmte Methode als eine andere zu verwenden (anrufen, eine WhatsApp-Nachricht senden, eine E-Mail senden usw.).**

			Bitte bewerten Sie anhand der Skala, inwiefern die jeweilige Aussage auf Sie zutrifft. Die Skala reicht von “Stimme überhaupt nicht zu” bis “Stimme voll zu”.
27*	coms_2	7-Punkt Likert-Skala (1 Stimme überhaupt nicht zu, 7 Stimme voll zu)	**Ich weiss, wie ich mit einem Smartphone eine beliebige Datei an einen Kontakt senden kann.** Bitte bewerten Sie anhand der Skala, inwiefern die jeweilige Aussage auf Sie zutrifft. Die Skala reicht von “Stimme überhaupt nicht zu” bis “Stimme voll zu”.
28*	coms_3 (reverse)	7-Punkt Likert-Skala (1 Stimme überhaupt nicht zu, 7 Stimme voll zu)	**Egal, mit wem ich kommuniziere: Emojis sind immer praktisch.** Bitte bewerten Sie anhand der Skala, inwiefern die jeweilige Aussage auf Sie zutrifft. Die Skala reicht von “Stimme überhaupt nicht zu” bis “Stimme voll zu”.
			Teil 2: Manipulationscheck
29*	MP1 (Manipulations-check) (mp1_true) (mp1_vid) (mp1_nl) (mp1_none)	4-Punkt-Skala, Reihenfolge randomisiert.	**Bevor Sie mit der Umfrage gestartet haben, wurde Ihnen ein Hinweis in einem Pop-up Fenster angezeigt. Worum ging es bei diesem Hinweis?** – Um die Sammlung von Cookies – Um die Aufzeichnung Ihrer Session via Videoaufnahme – Um die Anmeldung zu einem Newsletter – Weiss nicht

30*	MP2 (Manipulations-check) Gruppe A: (mp2_ac) (mp2_aj) (mp2_dc) (mp2_none) (mp2_dk) Gruppe B: (mp2_ac) (mp2_dc) (mp2_none) (mp2_dk)	5- bzw. 4-Punkt-Skala, Reihenfolge randomisiert.	**Wie haben Sie auf den Hinweis geantwortet?** Gruppe A: - Alle zulassen - Auswahl erlauben - Ablehnen - Weiss nicht - Ich habe nicht darauf geantwortet Gruppe B: - Zulassen - Ablehnen - Weiss nicht - Ich habe nicht darauf geantwortet
			Teil 3: Erkennung von Dark Patterns
31* 32* 33*	DE de_1 de_2 (reverse) de_3	Bipolare 7-Punkt-Matrix	((Screenshot des Cookie-Hinweis der jeweiligen Gruppe)) **Bitte bewerten Sie die grafische Gestaltung des oben abgebildeten Cookie-Hinweis an der folgenden Skala.** - Klar = 1, Irreführend=7 - Trügerisch = 1, Vertrauenswürdig=7 - Sachlich = 1, Verzerrt=7

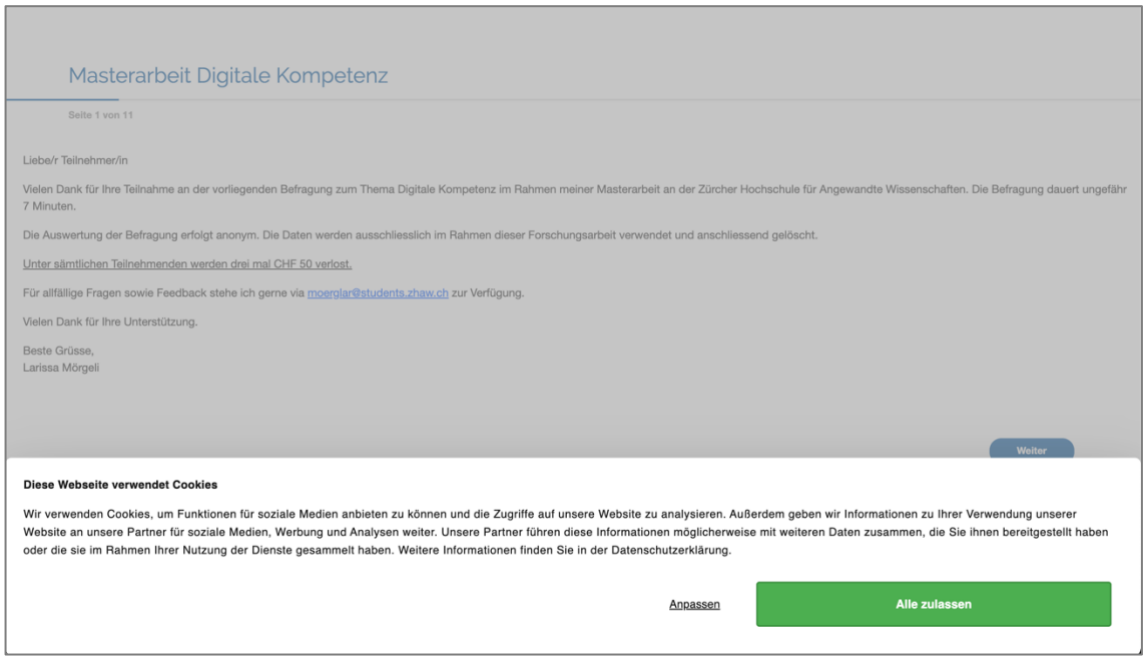
			Teil 4: Demografische Angaben
34*	ag	Texteingabe	**Bitte nennen Sie Ihr Alter in Jahren:**
35*	ge (f) (m) (b)	Single-Choice-Skala	**Bitte nennen Sie Ihr Geschlecht:** - weiblich - männlich - nichtbinär/drittes Geschlecht
36*	ed (ed_u) (ed_hf) (ed_bl) (ed_ma) (ed_os) (ed_other)	Single-Choice-Skala	**Bitte geben Sie ihre höchste abgeschlossene Ausbildung an:** - Hochschulabschluss (Universität, ETH, Fachhochschule oder gleichwertige Ausbildung) - höhere Berufsbildung (Meisterprüfung, eidg. Fachausweis, höhere Fachschule usw.) - Maturität (Gymnasiale Maturitätsschule oder Fachhochschule) - Berufslehre oder gleichwertige Ausbildung - Obligatorische Schulbildung (ohne nachobligatorische Ausbildung) - Anderes: ---
37*	oc_1 oc_oc oc_ne oc_ed oc_ap oc_hh oc_iv oc_ps	Single-Choice-Skala	**Welcher Beschäftigung gehen Sie aktuell (hauptsächlich) nach?** - Voll- oder Teilzeiterwerbstätig - Erwerbslos, auf Stellensuche - In einer schulischen Ausbildung, Studium - In einer Berufslehre - Kinderbetreuung / Haushalt / Familie - IV-Rentner/IV-Rentnerin

	oc_other		- AHV-Rentner/AHV-Rentnerin - Andere (bitte beschreiben) -
38	oc_2	Texteingabe	**Bitte nennen Sie Ihre aktuelle Berufsbezeichnung oder die der letzten Erwerbstätigkeit, sofern sie aktuell nicht erwerbstätig sind.** - Offenes Textfeld
39	fb	Texteingabe	**Sind bei der Beantwortung des Fragebogens Probleme aufgetaucht oder haben Sie sonstige Anregungen?**
40	co	Texteingabe	**Möchten Sie an der Verlosung des Gewinns teilnehmen?** Dann hinterlassen Sie bitte Ihre E-Mailadresse für die Kontaktaufnahme.
			Abschluss
-	-	Abschluss	Besten Dank für Ihre Teilnahme! Die Befragung ist nun zu Ende. Für allfällige Fragen sowie Feedback stehe ich gerne via [redacted] zur Verfügung.

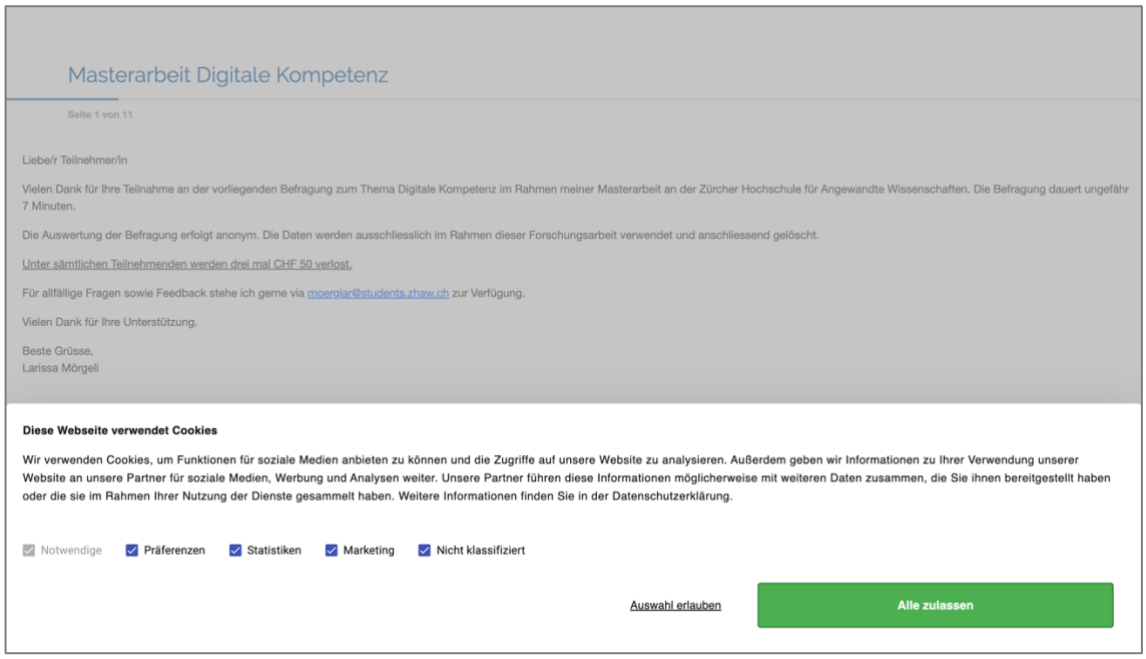
*= Beantwortung der Frage obligatorisch

7.2 Anhang B: Visualisierung der Einbettung des Cookie-Zustimmungshinweises in der Umfrage

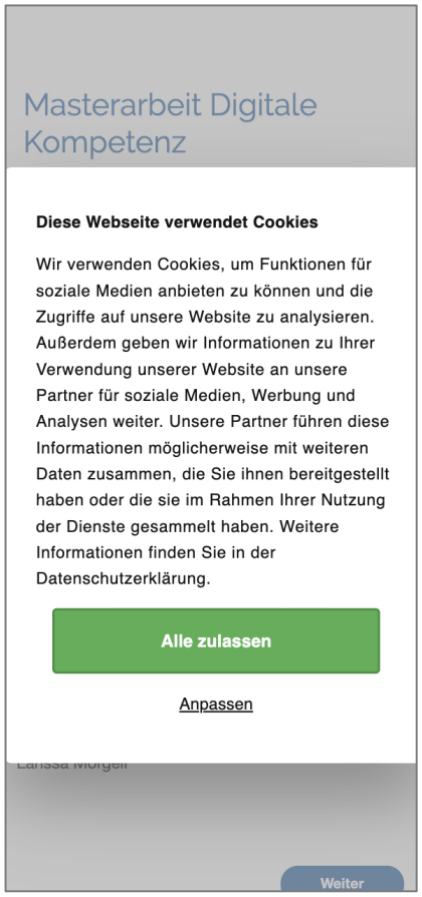
Visualisierung Cookie-Zustimmungshinweis der Gruppe A auf dem Desktopgerät – Teil 1



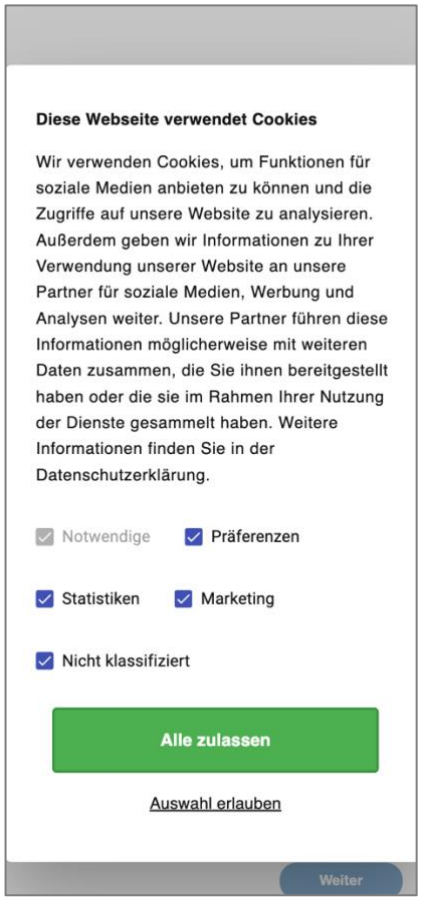
Visualisierung Cookie-Zustimmungshinweis der Gruppe A auf dem Desktopgerät – Teil 2



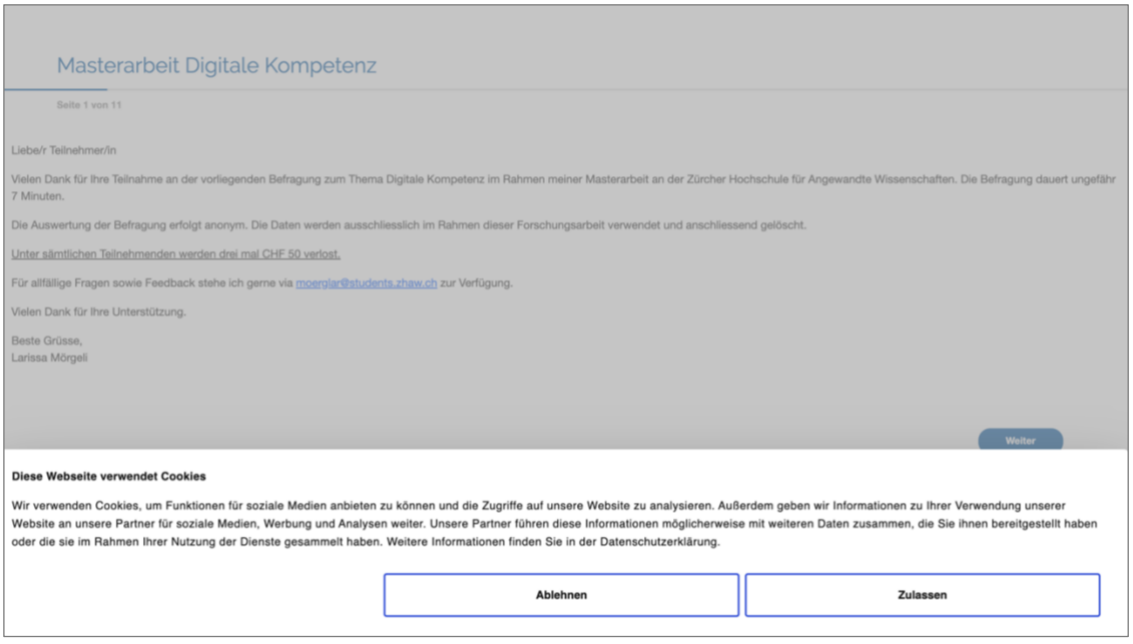
Visualisierung Cookie-Zustimmungshinweis der Gruppe A auf dem Mobilgerät – Teil 1



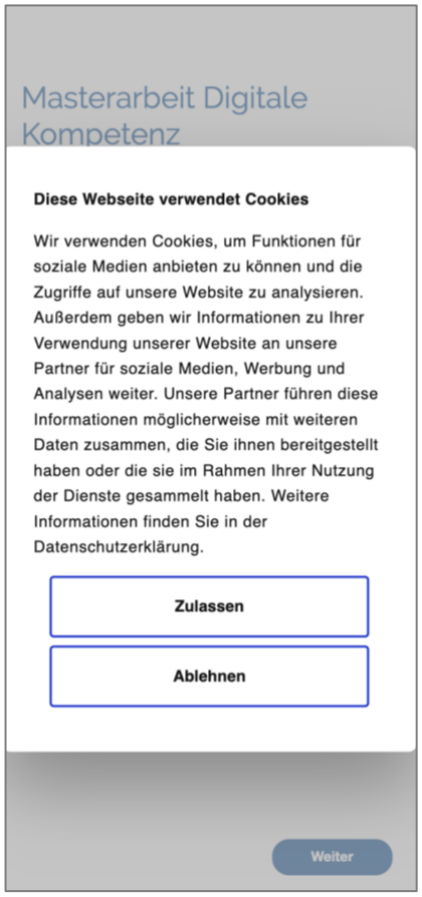
Visualisierung Cookie-Zustimmungshinweis der Gruppe A auf dem Mobilgerät – Teil 2



Visualisierung Cookie-Zustimmungshinweis der Gruppe B auf dem Desktopgerät



Visualisierung Cookie-Zustimmungshinweis der Gruppe B auf dem Mobilgerät



7.3 Anhang C: Übersetzung der Konstrukte

Faktor	Item	Item Englisch	Item übersetzt
Digital Literacy			
Technological skill (TS)	1	I know how to bookmark a website I like so I can view it later.	Ich weiss, wie ich eine Webseite, die mir gefällt, mit einem Lesezeichen versehe (oder als Favorit speichere), damit ich sie mir später ansehen kann.
	2	I always know how to download/save a photo I found online.	Ich weiss immer, wie ich ein Foto, das ich online gefunden habe, herunterladen/speichern kann.
	3	I know how to download information I found online.	Ich weiss, wie ich Informationen (bspw. Zeitungsartikel), die ich online gefunden habe, herunterladen kann.
	4	I always know how to connect to a Wi-Fi network, no matter the device or where I am.	Ich weiss immer, wie ich eine Verbindung zu einem WLAN-Netzwerk herstellen kann, unabhängig vom Gerät oder wo ich mich befinde.

	5	I know how to use shortcut keys (e.g. CTRL + C o cmd + C for copy).	Ich weiss, wie man Tastenkombinationen verwendet (z. B. CTRL + C, Strg + C oder cmd + C für kopieren).
	6	I do not like downloading apps for smartphones as I find difficult to learn how to use them.	Ich lade nicht gerne Apps für Smartphones herunter, da es mir schwer fällt, ihre Bedienung zu erlernen.
	7	If I want to install new programs on my computer, I will ask someone to do it for me because I do not know.	Wenn ich neue Programme auf meinem Computer installieren möchte, dann bitte ich jemanden, dies für mich zu tun, weil ich nicht weiss, wie es geht.
Personal security skill (PSS)	8	I know how to deactivate the function showing my geographical position (e.g. Facebook, apps).	Ich weiss, wie ich die Funktion zur Anzeige meiner geografischen Position deaktivieren kann (z. B. Facebook, Apps).
	9	I know when I can post pictures and videos of other people online.	Ich weiss, wann ich rechtlich gesehen Bilder und Videos von anderen Menschen online stellen darf.

	10	I know how to use ‘report abuse’ buttons on social media sites (e.g., someone uses my photo without my permission).	Ich weiss, wie man die «Missbrauch melden» Buttons auf sozialen Medien verwendet (z. B. wenn jemand mein Foto ohne meine Erlaubnis verwendet).
	11	I know how to change the sharing settings of social media to choose what others can see about me (friends of friends, friends only, only me).	Ich weiss, wie ich die Privatsphäre-Einstellungen auf den sozialen Medien anpassen kann, um festzulegen, was andere von mir sehen können (Freunde von Freunden, nur Freunde, nur ich).
Critical skill (CS)	12	I know how to compare different sources to decide if information is true.	Ich weiss, wie man verschiedene Quellen vergleichen kann, um zu entscheiden, ob die Informationen wahr sind.
	13	I know how to determine if the information I find online is reliable.	Ich weiss, wie ich feststellen kann, ob die Informationen, die ich online finde, zuverlässig sind.
	14	I know how to identify the author of the	Ich weiss, wie ich den Autor der Informationen identifizieren und ihre

		information and evaluate their reliability.	Zuverlässigkeit bewerten kann.
	15	I know how to compare different apps in order to choose which one is most reliable and secure.	Ich weiss, wie ich verschiedene Apps vergleichen kann, um auszuwählen, welche die zuverlässigste und sicherste ist.
	16	If I meet someone online, I know how to check if their profile is real.	Wenn ich jemanden online kennenlerne, weiss ich, wie ich überprüfen kann, ob sein Profil echt ist.
Devices security skill (DSS)	17	I use software to detect and remove viruses.	Ich verwende Software um Viren zu erkennen und entfernen.
	18	I know how to detect a virus in my digital device.	Ich weiss, wie ich einen Virus in meinem digitalen Gerät erkennen kann.
	19	I know how to block unwanted or junk mail/spam.	Ich weiss, wie man unerwünschte oder Junk-Mails/Spam blockiert.
	20	If something doesn't work occurs while I am using a device (computer, smartphone, etc.), I usually know	Wenn etwas nicht funktioniert, während ich ein Gerät (Computer, Smartphone usw.) benutze, weiss ich in der Regel, was

		what it is and how to fix the problem.	es ist und wie ich das Problem beheben kann.
Informational skill (IS)	21	I find hard to decide what the best keywords are for online searching.	Es fällt mir schwer zu entscheiden, welches die besten Suchbegriffe für die Online-Suche sind.
	22	I find confusing the way in which many websites are designed.	Ich finde die Art und Weise, wie viele Websites gestaltet sind, verwirrend.
	23	Sometimes I find difficult to determine how useful the information is for my purpose.	Manchmal fällt es mir schwer zu bestimmen, wie nützlich die Informationen, die ich online gefunden habe, für meine Zwecke sind.
	24	I get tired when looking for information online.	Ich werde schnell müde, wenn ich online nach Informationen suche.
	25	Sometimes I end up on websites without knowing how I got there.	Manchmal lande ich auf Websites, ohne zu wissen, wie ich dort hingekommen bin.
Communication skill (COMS)	26	Depending on who I want to communicate with, it is better to use one method over the	Je nachdem, mit wem ich kommunizieren möchte, ist es besser, eine bestimmte Methode als

		other (make a call, send a WhatsApp message, send an email, etc.)	eine andere zu verwenden (anrufen, eine WhatsApp-Nachricht senden, eine E-Mail senden usw.).
	27	I know how to send any file to a contact using a smartphone. No matter with who I communicate: emojis are always useful.	Ich weiss, wie ich mit einem Smartphone eine beliebige Datei an einen Kontakt senden kann.
	28	No matter with who I communicate: emojis are always useful.	Egal, mit wem ich kommuniziere: Emojis sind immer praktisch.
Wahrgenommene Täuschung / Erkennung von Dark Patterns			
Wahrgenommene Täuschung	1	Accurate – Misleading	Klar – Irreführend
	2	Truthful – Deceptive	Vertrauenswürdig – Trügerisch
	3	Factual – Distorted	Sachlich – Verzerrt

7.4 Anhang D: Deskriptive Analyse

7.4.1 Stichprobenanalyse Gesamt

Geschlecht					
		Häufigkeit	Prozent	Gültige Prozente	Kumulierte Prozente
Gültig	männlich	53	52.5	52.5	52.5
	weiblich	48	47.5	47.5	100.0
	Gesamt	101	100.0	100.0	

Alter					
	N	Minimum	Maximum	Mittelwert	Std.-Abweichung
Alter	101	22	79	42.04	16.226
Gültige Werte (listenweise)	101				

Altersgruppen					
		Häufigkeit	Prozent	Gültige Prozente	Kumulierte Prozente
Gültig	20-39 Jahre	55	54.5	54.5	54.5
	40-64 Jahre	33	32.7	32.7	87.1
	65-79 Jahre	13	12.9	12.9	100.0
	Gesamt	101	100.0	100.0	

Ausbildung					
		Häufigkeit	Prozent	Gültige Prozente	Kumulierte Prozente
Gültig	Anderes	1	1.0	1.0	1.0
	Maturität	8	7.9	7.9	8.9
	Berufslehre	23	22.8	22.8	31.7
	höhere Berufsbildung	26	25.7	25.7	57.4
	Hochschulabschluss	43	42.6	42.6	100.0
	Gesamt	101	100.0	100.0	

Beschäftigung					
		Häufigkeit	Prozent	Gültige Prozente	Kumulierte Prozente
Gültig	Andere	2	2.0	2.0	2.0
	AHV-Rente	11	10.9	10.9	12.9
	IV-Rente	2	2.0	2.0	14.9
	Kinderbetreuung/Haushalt/Familie	4	4.0	4.0	18.8
	schulischen Ausbildung, Studium	11	10.9	10.9	29.7
	Voll- oder Teilzeiterwerbstätig	71	70.3	70.3	100.0
	Gesamt	101	100.0	100.0	

Digitale Kompetenz					
Mittelwert	N	Std.-Abweichung	Median	Minimum	Maximum
5.2007	101	1.12888	5.4679	1.48	7.00

Dimensionen der Digitalen Kompetenz						
	Technologische Fertigkeiten	Persönliche Sicherheitskompetenz	Kritische Analyse-Fertigkeit	Geräte-Sicherheitskompetenz	Informationskompetenz	Kommunikationsfertigkeit
Mittelwert	5.8260	5.0767	4.4277	4.8787	4.9406	6.0545
N	101	101	101	101	101	101
Std.-Abweichung	1.19174	1.53042	1.76613	1.38004	1.30768	1.08375
Median	6.1429	5.5000	4.8000	5.2500	5.2000	6.0000
Minimum	2.00	1.00	1.00	1.00	1.40	2.00
Maximum	7.00	7.00	7.00	7.00	7.00	7.00

Deskriptive Statistik – Digitale Kompetenz		
	Statistik	Standard Fehler

Digitale Kompetenz	Mittelwert		5.2007	.11233
	95% Konfidenzintervall des Mittelwerts	Untergrenze	4.9779	
		Obergrenze	5.4236	
	5% getrimmtes Mittel		5.2636	
	Median		5.4679	
	Varianz		1.274	
	Standard Abweichung		1.12888	
	Minimum		1.48	
	Maximum		7.00	
	Spannweite		5.52	
	Interquartilbereich		1.65	
	Schiefe		-.828	.240
	Kurtosis		.348	.476

Tests auf Normalverteilung						
	Kolmogorov-Smirnov[a]			Shapiro-Wilk		
	Statistik	df	Signifikanz	Statistik	df	Signifikanz
Digitale Kompetenz	.126	101	<.001	.945	101	<.001
a. Signifikanzkorrektur nach Lilliefors						

7.4.1 Stichprobenanalyse nach Gruppe

Geschlecht						
Gruppe			Häufigkeit	Prozent	Gültige Prozente	Kumulierte Prozente
Experimental-gruppe	Gültig	männlich	20	44.4	44.4	44.4
		weiblich	25	55.6	55.6	100.0
		Gesamt	45	100.0	100.0	
Kontroll-gruppe	Gültig	männlich	33	58.9	58.9	58.9
		weiblich	23	41.1	41.1	100.0
		Gesamt	56	100.0	100.0	

Alter						
Gruppe		N	Minimum	Maximum	Mittel-wert	Std.-Abweichung
Experimental-gruppe	Alter	45	22	76	40.29	16.046
	Gültige Werte (listenweise)	45				
Kontroll-gruppe	Alter	56	24	79	43.45	16.377
	Gültige Werte (listenweise)	56				

Altersgruppen						
Gruppe			Häufigkeit	Prozent	Gültige Prozente	Kumulierte Prozente
Experimental-gruppe	Gültig	20-39 Jahre	27	60.0	60.0	60.0
		40-64 Jahre	13	28.9	28.9	88.9
		65-79 Jahre	5	11.1	11.1	100.0
		Gesamt	45	100.0	100.0	
Kontroll-gruppe	Gültig	20-39 Jahre	28	50.0	50.0	50.0
		40-64 Jahre	20	35.7	35.7	85.7
		65-79 Jahre	8	14.3	14.3	100.0
		Gesamt	56	100.0	100.0	

Ausbildung						
Gruppe			Häufigkeit	Prozent	Gültige Prozente	Kumulierte Prozente
Experimental-gruppe	Gültig	Anderes	1	2.2	2.2	2.2
		Maturität	2	4.4	4.4	6.7
		Berufslehre	12	26.7	26.7	33.3
		höhere Berufsbildung	13	28.9	28.9	62.2
		Hochschulabschluss	17	37.8	37.8	100.0
		Gesamt	45	100.0	100.0	
Kontroll-gruppe	Gültig	Maturität	6	10.7	10.7	10.7
		Berufslehre	11	19.6	19.6	30.4
		höhere Berufsbildung	13	23.2	23.2	53.6
		Hochschulabschluss	26	46.4	46.4	100.0
		Gesamt	56	100.0	100.0	

Beschäftigung						
Gruppe			Häufigkeit	Prozent	Gültige Prozente	Kumulierte Prozente
Experimental-gruppe	Gültig	AHV-Rente	4	8.9	8.9	8.9
		IV-Rente	2	4.4	4.4	13.3

		Kinderbetreuung/Haushalt/Familie	1	2.2	2.2	15.6
		schulischen Ausbildung, Studium	6	13.3	13.3	28.9
		Voll- oder Teilzeiterwerbstätig	32	71.1	71.1	100.0
		Gesamt	45	100.0	100.0	
Kontroll-gruppe	Gültig	AHV-Rente	8	14.3	14.3	14.3
		Kinderbetreuung/Haushalt/Familie	3	5.4	5.4	19.6
		schulischen Ausbildung, Studium	5	8.9	8.9	28.6
		Voll- oder Teilzeiterwerbstätig	40	71.4	71.4	100.0
		Gesamt	56	100.0	100.0	

Digitale Kompetenz						
Gruppe	Mittelwert	N	Std.-Abweichung	Median	Minimum	Maximum
Experimental-gruppe	5.2652	45	.93990	5.5714	3.22	7.00
Kontrollgruppe	5.1489	56	1.26656	5.4601	1.48	6.83
Insgesamt	5.2007	101	1.12888	5.4679	1.48	7.00

Dimensionen der Digitalen Kompetenz							
Gruppe		Technologische Fertigkeiten	Persönliche Sicherheits-kompetenz	Kritische Analyse-Fertigkeit	Geräte-Sicherheits-kompetenz	Informations-kompetenz	Kommunikation sfertigkeit
Experimental-gruppe	Mittelwert	5.9714	5.2444	4.3911	4.9444	4.9289	6.1111
	N	45	45	45	45	45	45
	Std.-Abweichung	1.01455	1.32662	1.59371	1.28462	1.16475	.94682
	Median	6.2857	5.7500	4.8000	5.2500	5.2000	6.0000
	Minimum	2.71	1.00	1.00	1.75	1.80	3.50
	Maximum	7.00	7.00	7.00	7.00	7.00	7.00
Kontroll-gruppe	Mittelwert	5.7092	4.9420	4.4571	4.8259	4.9500	6.0089
	N	56	56	56	56	56	56
	Std.-Abweichung	1.31439	1.67603	1.90720	1.46157	1.42255	1.18893
	Median	6.1429	5.1250	5.2000	5.0000	5.1000	6.0000
	Minimum	2.00	1.00	1.00	1.00	1.40	2.00
	Maximum	7.00	7.00	7.00	7.00	7.00	7.00
Insgesamt	Mittelwert	5.8260	5.0767	4.4277	4.8787	4.9406	6.0545
	N	101	101	101	101	101	101
	Std.-Abweichung	1.19174	1.53042	1.76613	1.38004	1.30768	1.08375
	Median	6.1429	5.5000	4.8000	5.2500	5.2000	6.0000
	Minimum	2.00	1.00	1.00	1.00	1.40	2.00
	Maximum	7.00	7.00	7.00	7.00	7.00	7.00

7.5 Anhang E: Statistische Verfahren

7.4.2 Cronbach Alpha

Digitale Kompetenz – Technologische Fertigkeiten

Zusammenfassung der Fallverarbeitung			
		N	%
Fälle	Gültig	101	100.0
	Ausgeschlossen[a]	0	.0
	Gesamt	101	100.0

a. Listenweise Löschung auf der Grundlage aller Variablen in der Prozedur.

Reliabilitätsstatistiken	
Cronbachs Alpha	Anzahl der Items
.861	7

Itemstatistiken			
	Mittelwert	Std.-Abweichung	N
surveyData/technological_skills/ts_1	6.12	1.545	101
surveyData/technological_skills/ts_2	6.11	1.295	101
surveyData/technological_skills/ts_3	5.77	1.434	101
surveyData/technological_skills/ts_4	5.96	1.574	101
surveyData/technological_skills/ts_5	5.84	1.567	101

surveyData/technological_skills/ts_6	5.73	1.691	101
surveyData/technological_skills/ts_7	5.25	2.080	101

Item-Skala-Statistiken				
	Skalenmittelwert, wenn Item weggelassen	Skalenvarianz, wenn Item weggelassen	Korrigierte Item-Skala-Korrelation	Cronbachs Alpha, wenn Item weggelassen
surveyData/technological_skills/ts_1	34.66	52.806	.642	.840
surveyData/technological_skills/ts_2	34.67	55.422	.648	.841
surveyData/technological_skills/ts_3	35.01	57.170	.478	.860
surveyData/technological_skills/ts_4	34.82	51.688	.681	.834
surveyData/technological_skills/ts_5	34.94	52.236	.658	.837
surveyData/technological_skills/ts_6	35.05	51.228	.641	.840
surveyData/technological_skills/ts_7	35.53	45.651	.698	.834

Skala-Statistiken			
Mittelwert	Varianz	Std.-Abweichung	Anzahl der Items
40.78	69.592	8.342	7

Digitale Kompetenz – Persönliche Sicherheitskompetenz

Zusammenfassung der Fallverarbeitung			
		N	%
Fälle	Gültig	101	100.0
	Ausgeschlossen[a]	0	.0

	Gesamt	101	100.0

a. Listenweise Löschung auf der Grundlage aller Variablen in der Prozedur.

Reliabilitätsstatistiken

Cronbachs Alpha	Anzahl der Items
.772	4

Itemstatistiken

	Mittelwert	Std.-Abweichung	N
surveyData/personal_security_skills/pss_1	5.55	1.884	101
surveyData/personal_security_skills/pss_2	4.59	1.888	101
surveyData/personal_security_skills/pss_3	4.75	2.206	101
surveyData/personal_security_skills/pss_4	5.41	1.950	101

Item-Skala-Statistiken

	Skalenmittelwert, wenn Item weggelassen	Skalenvarianz, wenn Item weggelassen	Korrigierte Item-Skala-Korrelation	Cronbachs Alpha, wenn Item weggelassen
surveyData/personal_security_skills/pss_1	14.75	23.208	.590	.709
surveyData/personal_security_skills/pss_2	15.71	25.907	.417	.792

surveyData/personal_security_skills/pss_3	15.55	19.830	.650	.674
surveyData/personal_security_skills/pss_4	14.90	21.790	.653	.675

Skala-Statistiken			
Mittelwert	Varianz	Std.-Abweichung	Anzahl der Items
20.31	37.475	6.122	4

Digitale Kompetenz – Kritische Analyse-Fertigkeit

Zusammenfassung der Fallverarbeitung			
		N	%
Fälle	Gültig	101	100.0
	Ausgeschlossen[a]	0	.0
	Gesamt	101	100.0

a. Listenweise Löschung auf der Grundlage aller Variablen in der Prozedur.

Reliabilitätsstatistiken	
Cronbachs Alpha	Anzahl der Items
.943	5

Itemstatistiken			
	Mittelwert	Std.-Abweichung	N
surveyData/critical_skills/cs_1	4.87	1.937	101
surveyData/critical_skills/cs_2	4.66	1.941	101

Digital Literacy Skala: critical_skills - cs_3	4.23	1.999	101
Digital Literacy Skala: critical_skills - cs_4	4.54	1.983	101
Digital Literacy Skala: critical_skills - cs_5	3.83	1.924	101

Item-Skala-Statistiken

	Skalenmittelwert, wenn Item weggelassen	Skalenvarianz, wenn Item weggelassen	Korrigierte Item-Skala-Korrelation	Cronbachs Alpha, wenn Item weggelassen
surveyData/critical_skills/cs_1	17.27	49.358	.914	.917
surveyData/critical_skills/cs_2	17.48	50.272	.870	.925
Digital Literacy Skala: critical_skills - cs_3	17.91	49.382	.875	.924
Digital Literacy Skala: critical_skills - cs_4	17.59	50.904	.818	.935
Digital Literacy Skala: critical_skills - cs_5	18.31	53.175	.752	.946

Skala-Statistiken

Mittelwert	Varianz	Std.-Abweichung	Anzahl der Items
22.14	77.981	8.831	5

Digitale Kompetenz – Geräte-Sicherheitskompetenz

Zusammenfassung der Fallverarbeitung			
		N	%
Fälle	Gültig	101	100.0
	Ausgeschlossen[a]	0	.0
	Gesamt	101	100.0

a. Listenweise Löschung auf der Grundlage aller Variablen in der Prozedur.

Reliabilitätsstatistiken	
Cronbachs Alpha	Anzahl der Items
.727	4

Itemstatistiken			
	Mittelwert	Std.-Abweichung	N
surveyData/devices_security_skills/dss_1	5.16	1.948	101
surveyData/devices_security_skills/dss_2	4.12	1.961	101
surveyData/devices_security_skills/dss_3	5.51	1.753	101
surveyData/devices_security_skills/dss_4	4.72	1.773	101

Item-Skala-Statistiken				
	Skalenmittelwert, wenn Item weggelassen	Skalenvarianz, wenn Item weggelassen	Korrigierte Item-Skala-Korrelation	Cronbachs Alpha, wenn

				Item weggelassen
surveyData/devices_security_skills/dss_1	14.36	21.932	.260	.812
surveyData/devices_security_skills/dss_2	15.40	16.642	.624	.598
surveyData/devices_security_skills/dss_3	14.00	18.400	.599	.621
surveyData/devices_security_skills/dss_4	14.79	17.826	.635	.599

Skala-Statistiken			
Mittelwert	Varianz	Std.-Abweichung	Anzahl der Items
19.51	30.472	5.520	4

Digitale Kompetenz – Informationskompetenz

Zusammenfassung der Fallverarbeitung			
		N	%
Fälle	Gültig	101	100.0
	Ausgeschlossen[a]	0	.0
	Gesamt	101	100.0

a. Listenweise Löschung auf der Grundlage aller Variablen in der Prozedur.

Reliabilitätsstatistiken	
Cronbachs Alpha	Anzahl der Items
.817	5

Itemstatistiken

	Mittelwert	Std.-Abweichung	N
surveyData/informational_skills/is_1	5.17	1.721	101
surveyData/informational_skills/is_2	4.53	1.758	101
surveyData/informational_skills/is_3	5.09	1.556	101
surveyData/informational_skills/is_4	4.77	1.810	101
surveyData/informational_skills/is_5	5.14	1.744	101

Item-Skala-Statistiken

	Skalenmittelwert, wenn Item weggelassen	Skalenvarianz, wenn Item weggelassen	Korrigierte Item-Skala-Korrelation	Cronbachs Alpha, wenn Item weggelassen
surveyData/informational_skills/is_1	19.53	27.791	.661	.766
surveyData/informational_skills/is_2	20.17	27.901	.633	.774
surveyData/informational_skills/is_3	19.61	30.259	.588	.788
surveyData/informational_skills/is_4	19.93	27.725	.616	.780
surveyData/informational_skills/is_5	19.56	29.368	.547	.800

Skala-Statistiken			
Mittelwert	Varianz	Std.-Abweichung	Anzahl der Items
24.70	42.751	6.538	5

Digitale Kompetenz – Kommunikationsfertigkeit

Zusammenfassung der Fallverarbeitung			
		N	%
Fälle	Gültig	101	100.0
	Ausgeschlossen[a]	0	.0
	Gesamt	101	100.0
a. Listenweise Löschung auf der Grundlage aller Variablen in der Prozedur.			

Reliabilitätsstatistiken	
Cronbachs Alpha	Anzahl der Items
.275	3

Itemstatistiken			
	Mittelwert	Std.-Abweichung	N
surveyData/communication_skills/coms_1	6.07	1.219	101
surveyData/communication_skills/coms_2	6.04	1.399	101
surveyData/communication_skills/coms_3	3.64	1.932	101

Item-Skala-Statistiken				
	Skalenmittelwert, wenn Item weggelassen	Skalenvarianz, wenn Item weggelassen	Korrigierte Item-Skala-Korrelation	Cronbachs Alpha, wenn Item weggelassen
surveyData/communication_skills/coms_1	9.68	5.499	.316	-.070[a]

surveyData/communication_skills/coms_2	9.71	5.767	.158	.191
surveyData/communication_skills/coms_3	12.11	4.698	.043	.534

a. Der Wert ist negativ aufgrund einer negativen mittleren Kovarianz zwischen den Items. Dies verstößt gegen die Annahmen über die Zuverlässigkeit des Modells. Sie sollten die Item-Kodierungen überprüfen.

Skala-Statistiken

Mittelwert	Varianz	Std.-Abweichung	Anzahl der Items
15.75	8.788	2.964	3

Erkennung Dark Patterns– Wahrgenommene Täuschung

Zusammenfassung der Fallverarbeitung

		N	%
Fälle	Gültig	101	100.0
	Ausgeschlossen[a]	0	.0
	Gesamt	101	100.0

a. Listenweise Löschung auf der Grundlage aller Variablen in der Prozedur.

Reliabilitätsstatistiken

Cronbachs Alpha	Anzahl der Items
.744	3

Itemstatistiken

	Mittelwert	Std.-Abweichung	N
1= klar, 7=irreführend	2.87	1.922	101

1= vertrauensürdig, 7=trügerisch	3.64	1.758	101
1= sachlich, 7=verzerrt	2.75	1.646	101

Item-Skala-Statistiken

	Skalenmittelwert, wenn Item weggelassen	Skalenvarianz, wenn Item weggelassen	Korrigierte Item-Skala-Korrelation	Cronbachs Alpha, wenn Item weggelassen
1= klar, 7=irreführend	6.40	8.582	.583	.648
1= vertrauensürdig, 7=trügerisch	5.62	10.437	.467	.773
1= sachlich, 7=verzerrt	6.51	9.312	.679	.543

Skala-Statistiken

Mittelwert	Varianz	Std.-Abweichung	Anzahl der Items
9.27	18.838	4.340	3

7.4.3 Konfirmatorische Faktorenanalyse

```
> library(lavaan)
> DL_model <- ' ts =~ ts_1 + ts_2 + ts_3 + ts_4 + ts_5 + R_ts_6 + R_ts_7
+             pss =~ pss_1 + pss_2 + pss_3 + pss_4
+             cs =~ cs_1 + cs_2 + cs_3 + cs_4 + cs_5
+             dss =~ dss_1 + dss_2 + dss_3 + dss_4
+             is =~ R_is_1 + R_is_2 + R_is_3 + R_is_4 + R_is_5
+             coms =~ coms_1 + coms_2
+             de=~ de_1 + R_de_2 + de_3
+             dl=~ts + pss + cs + dss + is + coms
+             '

> fit_DL <- cfa(DL_model, data=df)
> summary(fit_DL, fit.measures=TRUE)
lavaan 0.6-11 ended normally after 78 iterations

  Estimator                         ML
  Optimization method           NLMINB
  Number of model parameters        67

  Number of observations           101

Model Test User Model:

  Test statistic               570.573
  Degrees of freedom               398
  P-value (Chi-square)           0.000

Model Test Baseline Model:

  Test statistic              2228.810
  Degrees of freedom               435
```

P-value	0.000

User Model versus Baseline Model:

Comparative Fit Index (CFI)	0.904
Tucker-Lewis Index (TLI)	0.895

Loglikelihood and Information Criteria:

Loglikelihood user model (H0)	-5144.036
Loglikelihood unrestricted model (H1)	-4858.749
Akaike (AIC)	10422.071
Bayesian (BIC)	10597.284
Sample-size adjusted Bayesian (BIC)	10385.669

Root Mean Square Error of Approximation:

RMSEA	0.066
90 Percent confidence interval - lower	0.053
90 Percent confidence interval - upper	0.077
P-value RMSEA <= 0.05	0.022

Standardized Root Mean Square Residual:

SRMR	0.069

Parameter Estimates:

Standard errors	Standard
Information	Expected
Information saturated (h1) model	Structured

Latent Variables:

	Estimate	Std.Err	z-value	P(>|z|)
ts =~				
ts_1	1.000			
ts_2	0.789	0.117	6.754	0.000
ts_3	0.744	0.130	5.724	0.000
ts_4	1.049	0.141	7.417	0.000
ts_5	0.954	0.141	6.757	0.000
R_ts_6	1.015	0.152	6.660	0.000
R_ts_7	1.365	0.187	7.302	0.000
pss =~				
pss_1	1.000			
pss_2	0.645	0.146	4.416	0.000
pss_3	1.207	0.171	7.070	0.000
pss_4	1.192	0.151	7.883	0.000
cs =~				
cs_1	1.000			
cs_2	0.957	0.051	18.939	0.000
cs_3	0.943	0.059	15.981	0.000
cs_4	0.901	0.063	14.250	0.000
cs_5	0.787	0.072	10.998	0.000
dss =~				
dss_1	1.000			
dss_2	3.069	1.382	2.221	0.026
dss_3	2.942	1.315	2.237	0.025
dss_4	3.429	1.516	2.262	0.024
is =~				
R_is_1	1.000			
R_is_2	0.992	0.153	6.492	0.000
R_is_3	0.835	0.135	6.197	0.000
R_is_4	0.979	0.157	6.243	0.000

R_is_5	0.857	0.150	5.701	0.000
coms =~				
coms_1	1.000			
coms_2	2.347	0.608	3.861	0.000
de =~				
de_1	1.000			
R_de_2	0.689	0.143	4.821	0.000
de_3	1.099	0.228	4.816	0.000
dl =~				
ts	1.000			
pss	1.201	0.179	6.715	0.000
cs	1.437	0.184	7.823	0.000
dss	0.395	0.178	2.215	0.027
is	0.684	0.147	4.661	0.000
coms	0.419	0.116	3.619	0.000

Covariances:

	Estimate	Std.Err	z-value	P(>|z|)
de ~~				
dl	-0.063	0.163	-0.386	0.699

Variances:

	Estimate	Std.Err	z-value	P(>|z|)
.ts_1	1.111	0.172	6.443	0.000
.ts_2	0.883	0.134	6.592	0.000
.ts_3	1.344	0.197	6.809	0.000
.ts_4	1.078	0.170	6.351	0.000
.ts_5	1.291	0.196	6.591	0.000
.R_ts_6	1.539	0.233	6.617	0.000
.R_ts_7	1.953	0.305	6.401	0.000
.pss_1	1.727	0.271	6.369	0.000
.pss_2	2.786	0.402	6.931	0.000

.pss_3	2.215	0.354	6.257	0.000
.pss_4	1.226	0.225	5.450	0.000
.cs_1	0.266	0.073	3.648	0.000
.cs_2	0.565	0.102	5.537	0.000
.cs_3	0.891	0.144	6.180	0.000
.cs_4	1.091	0.170	6.426	0.000
.cs_5	1.530	0.227	6.743	0.000
.dss_1	3.556	0.503	7.068	0.000
.dss_2	1.912	0.298	6.411	0.000
.dss_3	1.300	0.211	6.152	0.000
.dss_4	0.744	0.162	4.580	0.000
.R_is_1	1.333	0.247	5.403	0.000
.R_is_2	1.486	0.265	5.603	0.000
.R_is_3	1.284	0.218	5.880	0.000
.R_is_4	1.713	0.293	5.841	0.000
.R_is_5	1.837	0.296	6.208	0.000
.coms_1	1.206	0.176	6.833	0.000
.coms_2	0.481	0.276	1.747	0.081
.de_1	1.838	0.420	4.375	0.000
.R_de_2	2.198	0.347	6.335	0.000
.de_3	0.486	0.405	1.199	0.230
.ts	0.083	0.057	1.453	0.146
.pss	0.102	0.101	1.013	0.311
.cs	1.039	0.198	5.239	0.000
.dss	0.019	0.020	0.959	0.337
.is	1.053	0.280	3.756	0.000
.coms	0.060	0.047	1.254	0.210
de	1.819	0.554	3.280	0.001
dl	1.168	0.291	4.011	0.000

```
> inspect(fit_DL,what="std")$lambda
      ts   pss    cs   dss    is  coms    de dl
```

ts_1 0.728 0.000 0.000 0.000 0.000 0.000 0.000 0
ts_2 0.685 0.000 0.000 0.000 0.000 0.000 0.000 0
ts_3 0.583 0.000 0.000 0.000 0.000 0.000 0.000 0
ts_4 0.749 0.000 0.000 0.000 0.000 0.000 0.000 0
ts_5 0.685 0.000 0.000 0.000 0.000 0.000 0.000 0
R_ts_6 0.675 0.000 0.000 0.000 0.000 0.000 0.000 0
R_ts_7 0.738 0.000 0.000 0.000 0.000 0.000 0.000 0
pss_1 0.000 0.713 0.000 0.000 0.000 0.000 0.000 0
pss_2 0.000 0.459 0.000 0.000 0.000 0.000 0.000 0
pss_3 0.000 0.735 0.000 0.000 0.000 0.000 0.000 0
pss_4 0.000 0.821 0.000 0.000 0.000 0.000 0.000 0
cs_1 0.000 0.000 0.964 0.000 0.000 0.000 0.000 0
cs_2 0.000 0.000 0.921 0.000 0.000 0.000 0.000 0
cs_3 0.000 0.000 0.880 0.000 0.000 0.000 0.000 0
cs_4 0.000 0.000 0.848 0.000 0.000 0.000 0.000 0
cs_5 0.000 0.000 0.763 0.000 0.000 0.000 0.000 0
dss_1 0.000 0.000 0.000 0.231 0.000 0.000 0.000 0
dss_2 0.000 0.000 0.000 0.706 0.000 0.000 0.000 0
dss_3 0.000 0.000 0.000 0.757 0.000 0.000 0.000 0
dss_4 0.000 0.000 0.000 0.872 0.000 0.000 0.000 0
R_is_1 0.000 0.000 0.000 0.000 0.738 0.000 0.000 0
R_is_2 0.000 0.000 0.000 0.000 0.717 0.000 0.000 0
R_is_3 0.000 0.000 0.000 0.000 0.682 0.000 0.000 0
R_is_4 0.000 0.000 0.000 0.000 0.687 0.000 0.000 0
R_is_5 0.000 0.000 0.000 0.000 0.624 0.000 0.000 0
coms_1 0.000 0.000 0.000 0.000 0.000 0.424 0.000 0
coms_2 0.000 0.000 0.000 0.000 0.000 0.867 0.000 0
de_1 0.000 0.000 0.000 0.000 0.000 0.000 0.705 0
R_de_2 0.000 0.000 0.000 0.000 0.000 0.000 0.531 0
de_3 0.000 0.000 0.000 0.000 0.000 0.000 0.905 0

7.4.4 Hypothesenprüfung H1: Dark Pattern – Zustimmung zu den Cookies

Test auf Binominalverteilung

groupId = Experimentalgruppe

Deskriptive Statistiken[a]					
	N	Mittelwert	Std.-Abweichung	Minimum	Maximum
Cookie_Akzeptanz_binär	45	.9111	.28780	.00	1.00
a. groupId = Experimentalgruppe					

Test auf Binomialverteilung[a]						
		Kategorie	N	Beobachteter Anteil	Testanteil	Exakte Sig. (2-seitig)
Cookie_Akzeptanz_binär	Gruppe 1	Akzeptiert	41	.91	.50	<.001
	Gruppe 2	Angepasst oder abgelehnt	4	.09		
	Gesamt		45	1.00		
a. groupId = Experimentalgruppe						

Test Unterschied Akzeptanz versus Ablehnung der Cookies – Kontrollgruppe

groupId = Kontrollgruppe

Deskriptive Statistiken[a]					
	N	Mittelwert	Std.-Abweichung	Minimum	Maximum
Cookie_Akzeptanz_binär	56	.8214	.38646	.00	1.00
a. groupId = Kontrollgruppe					

Test auf Binomialverteilung[a]						
		Kategorie	N	Beobachteter Anteil	Testanteil	Exakte Sig. (2-seitig)
Cookie_Akzeptanz_binär	Gruppe 1	Akzeptiert	46	.82	.50	<.001

	Gruppe 2	Angepasst oder abgelehnt	10	.18		
	Gesamt		56	1.00		
a. groupId = Kontrollgruppe						

Pearson-Chi-Quadrat-Test

Kreuztabellen

Zusammenfassung der Fallverarbeitung						
	Fälle					
	Gültig		Fehlend		Gesamt	
	N	Prozent	N	Prozent	N	Prozent
groubpid_binary * Cookie_Akzeptanz_binär	101	100.0%	0	0.0%	101	100.0%

groubpid_binary * Cookie_Akzeptanz_binär Kreuztabelle				
Anzahl				
		Cookie_Akzeptanz_binär		
		Angepasst oder abgelehnt	Akzeptiert	Gesamt
groubpid_binary	.00	10	46	56
	1.00	4	41	45
Gesamt		14	87	101

Chi-Quadrat-Tests					
	Wert	df	Asymptotische Signifikanz (zweiseitig)	Exakte Sig. (zweiseitig)	Exakte Sig. (einseitig)
Pearson-Chi-Quadrat	1.681[a]	1	.195		
Kontinuitätskorrektur[b]	1.014	1	.314		
Likelihood-Quotient	1.744	1	.187		
Exakter Test nach Fisher				.252	.157

Zusammenhang linear-mit-linear	1.664	1	.197		
Anzahl der gültigen Fälle	101				
a. 0 Zellen (.0%) haben eine erwartete Häufigkeit kleiner 5. Die minimale erwartete Häufigkeit ist 6.24.					
b. Wird nur für eine 2x2-Tabelle berechnet					

Symmetrische Maße

		Wert	Näherungsweise Signifikanz
Nominal- bzgl. Nominalmaß	Phi	.129	.195
	Cramer-V	.129	.195
Anzahl der gültigen Fälle		101	

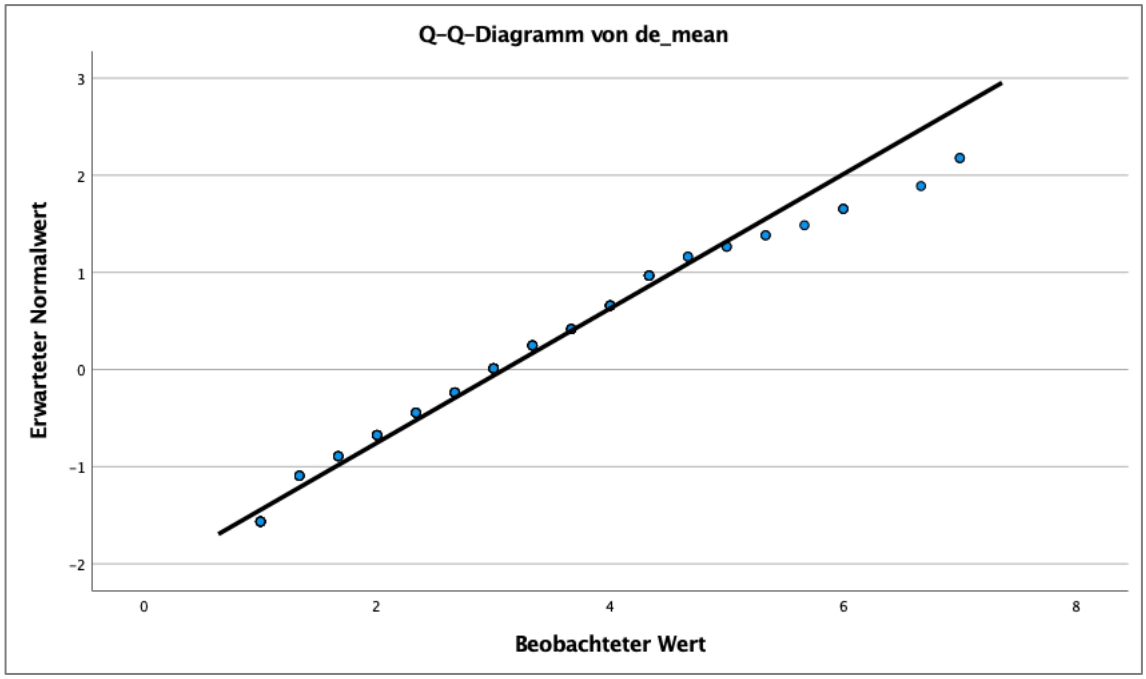
7.4.5 Hypothesenprüfung H2: Moderatoreffekt Erkennung von Dark Patterns

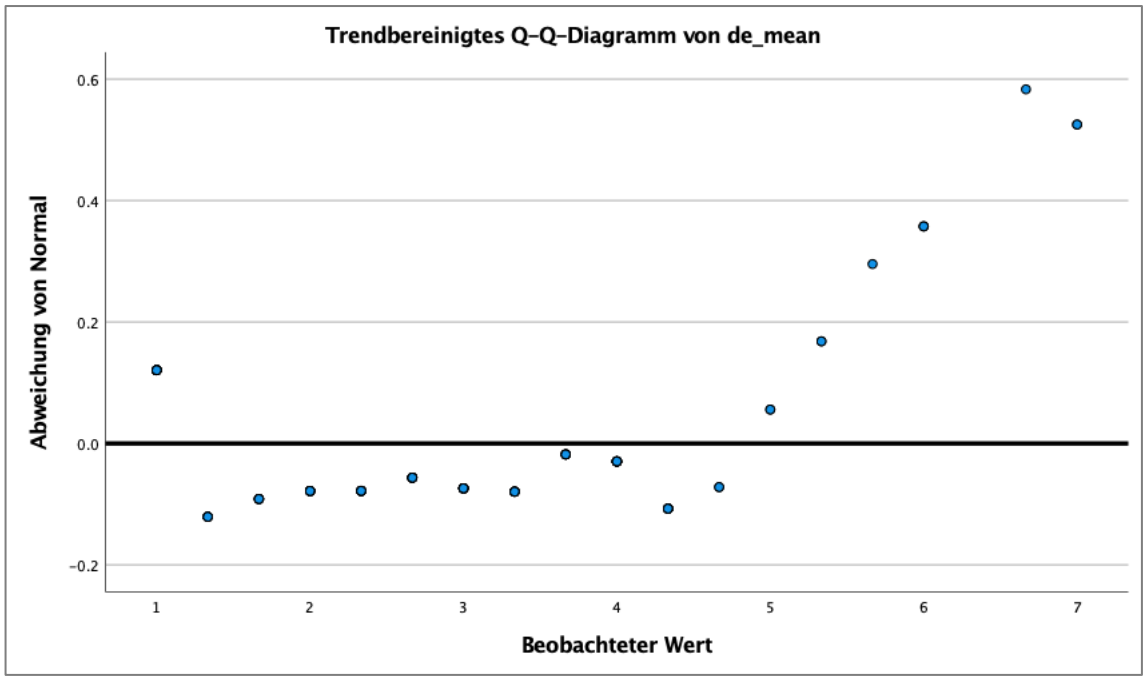
Test auf Normalverteilung

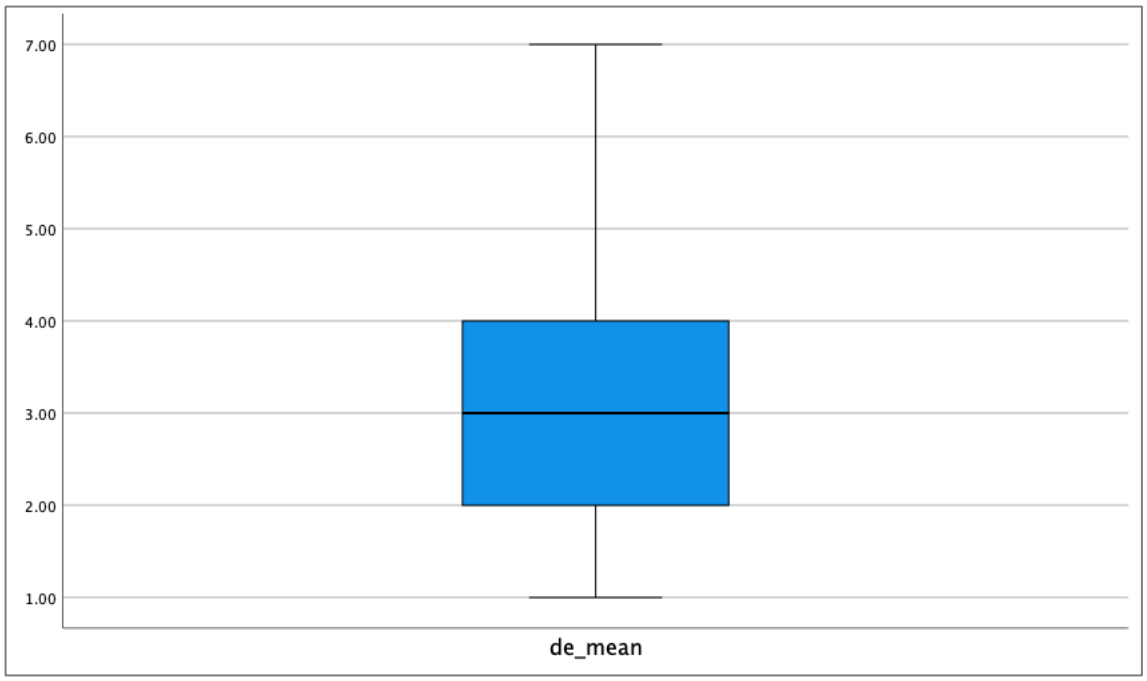
Verarbeitete Fälle						
	Fälle					
	Gültig		Fehlend		Gesamt	
	N	Prozent	N	Prozent	N	Prozent
de_mean	101	100.0%	0	0.0%	101	100.0%

Deskriptive Statistik				
			Statistik	Standard Fehler
de_mean	Mittelwert		3.0891	.14396
	95% Konfidenzintervall des Mittelwerts	Untergrenze	2.8035	
		Obergrenze	3.3747	
	5% getrimmtes Mittel		3.0141	
	Median		3.0000	
	Varianz		2.093	
	Standard Abweichung		1.44675	
	Minimum		1.00	
	Maximum		7.00	
	Spannweite		6.00	
	Interquartilbereich		2.00	
	Schiefe		.566	.240
	Kurtosis		.053	.476

Tests auf Normalverteilung						
	Kolmogorov-Smirnov[a]			Shapiro-Wilk		
	Statistik	df	Signifikanz	Statistik	df	Signifikanz
de_mean	.089	101	.047	.955	101	.002
a. Signifikanzkorrektur nach Lilliefors						


Q-Q-Diagramm von de_mean
Erwarteter Normalwert
Beobachteter Wert
3
2
1
0
-1
-2
0
2
4
6
8


Trendbereinigtes Q-Q-Diagramm von de_mean
Abweichung von Normal
Beobachteter Wert
0.6
0.4
0.2
0.0
-0.2
1
2
3
4
5
6
7



Mann-Whitney-Test

Ränge				
	groubpid_binary	N	Mittlerer Rang	Rangsumme
de_mean	.00	56	50.26	2814.50
	1.00	45	51.92	2336.50
	Gesamt	101		

Teststatistiken[a]	
	de_mean
Mann-Whitney-U-Test	1218.500
Wilcoxon-W	2814.500
Z	-.285
Asymp. Sig. (2-seitig)	.776
a. Gruppenvariable: groubpid_binary	

Moderationyanalyse

Run MATRIX procedure:

```
***************** PROCESS Procedure for SPSS Version 4.1 *****************

        Written by Andrew F. Hayes, Ph.D.       www.afhayes.com
    Documentation available in Hayes (2022). www.guilford.com/p/hayes3

**************************************************************************
****
Model  : 1
    Y  : Cookie_A
    X  : groubpid
    W  : de_mean

Sample
Size:  101

**************************************************************************
****
OUTCOME VARIABLE:
 Cookie_A

Coding of binary Y for logistic regression analysis:
  Cookie_A  Analysis
      .00       .00
     1.00      1.00

Model Summary
      -2LL    ModelLL        df         p   McFadden   CoxSnell   Nagelkrk
   79.3278     1.9649     3.0000      .5797      .0242      .0193      .0348

Model
             coeff         se          Z         p       LLCI       ULCI
constant     1.5358      .3520     4.3628      .0000      .8459     2.2257
```

groubpid .7951 .6339 1.2542 .2098 -.4474 2.0375
de_mean .0803 .2695 .2980 .7657 -.4480 .6086
Int_1 .0450 .4443 .1012 .9194 -.8259 .9159

These results are expressed in a log-odds metric.

Product terms key:
Int_1 : groubpid x de_mean

Likelihood ratio test(s) of highest order
unconditional interactions(s):
Chi-sq df p
X*W .0103 1.0000 .9191

Focal predict: groubpid (X)
Mod var: de_mean (W)

Data for visualizing the conditional effect of the focal predictor:
Paste text below into a SPSS syntax window and execute to produce plot.

```
DATA LIST FREE/
  groubpid   de_mean    Cookie_A   prob       .
BEGIN DATA.
     .0000    -1.4468     1.4196      .8053
    1.0000    -1.4468     2.1496      .8956
     .0000      .0000     1.5358      .8229
    1.0000      .0000     2.3309      .9114
     .0000     1.4468     1.6520      .8392
    1.0000     1.4468     2.5121      .9250
END DATA.
GRAPH/SCATTERPLOT=
 de_mean  WITH     Cookie_A BY       groubpid .
```

```
GRAPH/SCATTERPLOT=
 de_mean  WITH     prob     BY       groubpid .

*********************          ANALYSIS          NOTES          AND          ERRORS
*********************

Level of confidence for all confidence intervals in output:
  95.0000

NOTE: The following variables were mean centered prior to analysis:
        de_mean

WARNING: Variables names longer than eight characters can produce incorrect output
when some variables in the data file have the same first eight characters. Shorter
variable names are recommended. By using this output, you are accepting all risk
and consequences of interpreting or reporting results that may be incorrect.

------ END MATRIX -----
```

7.4.6 Hypothesenprüfung H3a: Digitale Kompetenz – Erkennung von Dark Patterns

Deskriptive Statistik

Deskriptive Statistiken[a]

	N	Minimum	Maximum	Mittelwert	Std.-Abweichung	Varianz	Schiefe		Kurtosis	
	Statistik	Statistik	Statistik	Statistik	Statistik	Statistik	Statistik	Std.-Fehler	Statistik	Std.-Fehler
1= klar, 7=irreführend	45	1	7	3.20	2.029	4.118	.415	.354	-1.172	.695
1= vertrauensürdig, 7=trügerisch	45	1	7	3.44	1.589	2.525	.426	.354	-.460	.695
1= sachlich, 7=verzerrt	45	1	7	2.91	1.743	3.037	.897	.354	.191	.695
de_mean	45	1.00	7.00	3.1852	1.59949	2.558	.726	.354	.081	.695
Gültige Werte (listenweise)	45									

a. groupId = Experimentalgruppe

Einfaktorielle ANOVA

groupId = Experimentalgruppe

Aufgenommene/Entfernte Variablen[a,b]

Modell	Aufgenommene Variablen	Entfernte Variablen	Methode
1	Digitale Kompetenz[c]	.	Einschluß

a. groupId = Experimentalgruppe

b. Abhängige Variable: de_mean

c. Alle gewünschten Variablen wurden eingegeben.

Modellzusammenfassung[a,c]				
Modell	R	R-Quadrat	Korrigiertes R-Quadrat	Standardfehler des Schätzers
1	.015[b]	.000	-.023	1.61779
a. groupId = Experimentalgruppe				
b. Einflußvariablen : (Konstante), Digitale Kompetenz				
c. Abhängige Variable: de_mean				

ANOVA[a,b]						
Modell		Quadratsumme	df	Mittel der Quadrate	F	Sig.
1	Regression	.026	1	.026	.010	.921[c]
	Nicht standardisierte Residuen	112.542	43	2.617		
	Gesamt	112.568	44			
a. groupId = Experimentalgruppe						
b. Abhängige Variable: de_mean						
c. Einflußvariablen : (Konstante), Digitale Kompetenz						

Koeffizienten[a,b]										
Modell		Nicht standardisierte Koeffizienten		Standardisierte Koeffizienten	T	Sig.	95.0% Konfidenzintervalle für B		Kollinearitätsstatistik	
		Regressionskoeffizient B	Std.-Fehler	Beta			Untergrenze	Obergrenze	Toleranz	VIF
1	(Konstante)	3.322	1.387		2.394	.021	.524	6.119		
	Digitale Kompetenz	-.026	.259	-.015	-.100	.921	-.549	.497	1.000	1.000
a. groupId = Experimentalgruppe										
b. Abhängige Variable: de_mean										

7.4.6 Hypothesenprüfung H3b: Moderator Effekt Digitaler Kompetenz

Moderationsanalyse

Run MATRIX procedure:

**** PROCESS Procedure for SPSS Version 4.1 ****

Written by Andrew F. Hayes, Ph.D. www.afhayes.com
Documentation available in Hayes (2022). www.guilford.com/p/hayes3

****
****
Model : 1
Y : Cookie_A
X : groubpid
W : dl_mean

Sample
Size: 101

****
****
OUTCOME VARIABLE:
Cookie_A

Coding of binary Y for logistic regression analysis:
Cookie_A Analysis
.00 .00
1.00 1.00

Model Summary
-2LL ModelLL df p McFadden CoxSnell Nagelkrk

78.6662 2.6266 3.0000 .4529 .0323 .0257 .0464

Model

	coeff	se	Z	p	LLCI	ULCI
constant	1.5247	.3490	4.3689	.0000	.8407	2.2088
groubpid	.8632	.6556	1.3168	.1879	-.4217	2.1481
dl_mean	-.0456	.2827	-.1613	.8718	-.5996	.5084
Int_1	.5530	.6171	.8962	.3702	-.6565	1.7626

These results are expressed in a log-odds metric.

Product terms key:

Int_1 : groubpid x dl_mean

Likelihood ratio test(s) of highest order unconditional interactions(s):

	Chi-sq	df	p
X*W	.8097	1.0000	.3682

Focal predict: groubpid (X)

Mod var: dl_mean (W)

Data for visualizing the conditional effect of the focal predictor:

Paste text below into a SPSS syntax window and execute to produce plot.

```
DATA LIST FREE/
  groubpid   dl_mean    Cookie_A   prob       .
BEGIN DATA.
     .0000    -1.1289     1.5762      .8287
    1.0000    -1.1289     1.8151      .8600
     .0000      .0000     1.5247      .8212
    1.0000      .0000     2.3880      .9159
```

```
     .0000     1.1289     1.4733      .8136
    1.0000     1.1289     2.9608      .9508
END DATA.
GRAPH/SCATTERPLOT=
 dl_mean  WITH     Cookie_A BY       groubpid .
GRAPH/SCATTERPLOT=
 dl_mean  WITH     prob     BY       groubpid .

************************        ANALYSIS        NOTES        AND        ERRORS
************************

Level of confidence for all confidence intervals in output:
  95.0000

NOTE: The following variables were mean centered prior to analysis:
         dl_mean

WARNING: Variables names longer than eight characters can produce incorrect output
when some variables in the data file have the same first eight characters. Shorter
variable names are recommended. By using this output, you are accepting all risk
and consequences of interpreting or reporting results that may be incorrect.

------ END MATRIX -----
```

7.4.6 Hypothesenprüfung H3c: Digitale Kompetenz – Zustimmung zu den Cookies

Logistische Regression

Zusammenfassung der Fallverarbeitung			
Ungewichtete Fälle[a]		N	Prozent
Ausgewählte Fälle	Einbezogen in Analyse	101	100.0
	Fehlende Fälle	0	.0
	Gesamt	101	100.0
Nicht ausgewählte Fälle		0	.0
Gesamt		101	100.0
a. Wenn die Gewichtung wirksam ist, finden Sie die Gesamtzahl der Fälle in der Klassifizierungstabelle.			

Codierung abhängiger Variablen	
Ursprünglicher Wert	Interner Wert
Angepasst oder abgelehnt	0
Akzeptiert	1

Block 0: Anfangsblock

Iterationsprotokoll[a,b,c]			
Iteration		-2 Log-Likelihood	Koeffizienten Konstante
Schritt 0	1	83.213	1.446
	2	81.316	1.783
	3	81.293	1.826
	4	81.293	1.827
a. Konstante in das Modell einbezogen.			
b. Anfängliche -2 Log-Likelihood: 81.293			

c. Schätzung beendet bei Iteration Nummer 4, weil die Parameterschätzer sich um weniger als .001 änderten.

Klassifizierungstabelle[a,b]

			Vorhergesagt		
			Cookie_Akzeptanz_binär		
	Beobachtet		Angepasst oder abgelehnt	Akzeptiert	Prozentsatz der Richtigen
Schritt 0	Cookie_Akzeptanz_binär	Angepasst oder abgelehnt	0	14	.0
		Akzeptiert	0	87	100.0
	Gesamtprozentsatz				86.1

a. Konstante in das Modell einbezogen.

b. Der Trennwert lautet .500

Variablen in der Gleichung

		RegressionskoeffizientB	Standardfehler	Wald	df	Sig.	Exp(B)
Schritt 0	Konstante	1.827	.288	40.247	1	<.001	6.214

Variablen nicht in der Gleichung

			Wert	df	Sig.
Schritt 0	Variablen	Digitale Kompetenz	.120	1	.729
	Gesamtstatistik		.120	1	.729

Block 1: Methode = Einschluß

Iterationsprotokoll[a,b,c,d]				
Iteration		-2 Log-Likelihood	Koeffizienten	
			Konstante	Digitale Kompetenz
Schritt 1	1	83.133	1.225	.042
	2	81.201	1.388	.076
	3	81.175	1.381	.086
	4	81.175	1.380	.087
a. Methode: Einschluß				
b. Konstante in das Modell einbezogen.				
c. Anfängliche -2 Log-Likelihood: 81.293				
d. Schätzung beendet bei Iteration Nummer 4, weil die Parameterschätzer sich um weniger als .001 änderten.				

Omnibus-Tests der Modellkoeffizienten				
		Chi-Quadrat	df	Sig.
Schritt 1	Schritt	.118	1	.731
	Block	.118	1	.731
	Modell	.118	1	.731

Modellzusammenfassung			
Schritt	-2 Log-Likelihood	Cox & Snell R-Quadrat	Nagelkerkes R-Quadrat
1	81.175[a]	.001	.002
a. Schätzung beendet bei Iteration Nummer 4, weil die Parameterschätzer sich um weniger als .001 änderten.			

Klassifizierungstabelle[a]		
	Beobachtet	Vorhergesagt

			Cookie_Akzeptanz_binär		Prozentsatz der Richtigen
			Angepasst oder abgelehnt	Akzeptiert	
Schritt 1	Cookie_Akzeptanz_binär	Angepasst oder abgelehnt	0	14	.0
		Akzeptiert	0	87	100.0
	Gesamtprozentsatz				86.1

a. Der Trennwert lautet .500

Variablen in der Gleichung

		Regressionskoeffizient B	Standardfehler	Wald	df	Sig.	Exp(B)
Schritt 1[a]	Digitale Kompetenz	.087	.250	.120	1	.729	1.090
	Konstante	1.380	1.311	1.109	1	.292	3.976

Variablen in der Gleichung

		95% Konfidenzintervall für EXP(B)	
		Unterer Wert	Oberer Wert
Schritt 1[a]	Digitale Kompetenz	.668	1.779
	Konstante		

a. In Schritt 1 eingegebene Variablen: Digitale Kompetenz.

Mediansplit Pearson-Chi-Quadrat-Test

Zusammenfassung der Fallverarbeitung

	Fälle		
	Gültig	Fehlend	Gesamt

	N	Prozent	N	Prozent	N	Prozent
Digitale Kompetenz (Binned) * Cookie_Akzeptanz_binär	101	100.0%	0	0.0%	101	100.0%

Digitale Kompetenz (Binned) * Cookie_Akzeptanz_binär Kreuztabelle

			Cookie_Akzeptanz_binär		
			Angepasst oder abgelehnt	Akzeptiert	Gesamt
Digitale Kompetenz (Binned)	Niedrig	Anzahl	7	43	50
		Erwartete Anzahl	6.9	43.1	50.0
		% von Digitale Kompetenz (Binned)	14.0%	86.0%	100.0%
	Hoch	Anzahl	7	44	51
		Erwartete Anzahl	7.1	43.9	51.0
		% von Digitale Kompetenz (Binned)	13.7%	86.3%	100.0%
Gesamt		Anzahl	14	87	101
		Erwartete Anzahl	14.0	87.0	101.0
		% von Digitale Kompetenz (Binned)	13.9%	86.1%	100.0%

Chi-Quadrat-Tests

	Wert	df	Asymptotische Signifikanz (zweiseitig)	Exakte Sig. (zweiseitig)	Exakte Sig. (einseitig)
Pearson-Chi-Quadrat	.002[a]	1	.968		
Kontinuitätskorrektur[b]	.000	1	1.000		
Likelihood-Quotient	.002	1	.968		
Exakter Test nach Fisher				1.000	.597
Zusammenhang linear-mit-linear	.002	1	.968		
Anzahl der gültigen Fälle	101				

a. 0 Zellen (.0%) haben eine erwartete Häufigkeit kleiner 5. Die minimale erwartete Häufigkeit ist 6.93.
b. Wird nur für eine 2x2-Tabelle berechnet

7.4.7 Explorative Analysen

Zusammenhang Dark Pattern – Manipulationscheck 2: Pearson-Chi-Quadrat-Test

Kreuztabellen

Zusammenfassung der Fallverarbeitung

	Fälle					
	Gültig		Fehlend		Gesamt	
	N	Prozent	N	Prozent	N	Prozent
groupId * mp2_recoded	76	100.0%	0	0.0%	76	100.0%

groupId * mp2_recoded Kreuztabelle

			mp2_recoded			
			Falschangabe	Korrekte Antwort	"Weiss nicht"	Gesamt
groupId	Experimental-gruppe	Anzahl	10	22	1	33
		Erwartete Anzahl	4.8	27.8	.4	33.0
		% von groupId	30.3%	66.7%	3.0%	100.0%
	Kontroll-gruppe	Anzahl	1	42	0	43
		Erwartete Anzahl	6.2	36.2	.6	43.0
		% von groupId	2.3%	97.7%	0.0%	100.0%
Gesamt		Anzahl	11	64	1	76
		Erwartete Anzahl	11.0	64.0	1.0	76.0
		% von groupId	14.5%	84.2%	1.3%	100.0%

Chi-Quadrat-Tests

	Wert	df	Asymptotische Signifikanz (zweiseitig)	Exakte Sig. (zweiseitig)
Pearson-Chi-Quadrat	13.532[a]	2	.001	<.001
Likelihood-Quotient	14.970	2	<.001	.001

Exakter Test nach Fisher-Freeman-Halton	13.527			<.001
Anzahl der gültigen Fälle	76			
a. 3 Zellen (50.0%) haben eine erwartete Häufigkeit kleiner 5. Die minimale erwartete Häufigkeit ist .43.				

Zusammenhang Beschäftigung – Akzeptanz der Cookies: Pearson-Chi-Quadrat-Test

Kreuztabellen

Zusammenfassung der Fallverarbeitung						
	Fälle					
	Gültig		Fehlend		Gesamt	
	N	Prozent	N	Prozent	N	Prozent
Cookie_Akzeptanz_binär * Beschäftigungsart	101	100.0%	0	0.0%	101	100.0%

Cookie_Akzeptanz_binär * Beschäftigungsart Kreuztabelle								
			Beschäftigungsart						Gesamt
			oc-ed	oc-hh	oc-iv	oc-oc	oc-ps	other	
Cookie_Akzeptanz_binär	Angepasst oder abgelehnt	Anzahl	0	0	1	12	1	0	14
		Erwartete Anzahl	1.5	.6	.3	9.8	1.5	.3	14.0
		% von Cookie_Akzeptanz_binär	0.0%	0.0%	7.1%	85.7%	7.1%	0.0%	100.0%
	Akzeptiert	Anzahl	11	4	1	59	10	2	87
		Erwartete Anzahl	9.5	3.4	1.7	61.2	9.5	1.7	87.0
		% von Cookie_Akzeptanz_binär	12.6%	4.6%	1.1%	67.8%	11.5%	2.3%	100.0%
Gesamt		Anzahl	11	4	2	71	11	2	101
		Erwartete Anzahl	11.0	4.0	2.0	71.0	11.0	2.0	101.0
		% von Cookie_Akzeptanz_binär	10.9%	4.0%	2.0%	70.3%	10.9%	2.0%	100.0%

Chi-Quadrat-Tests			
	Wert	df	Asymptotische Signifikanz (zweiseitig)
Pearson-Chi-Quadrat	5.682[a]	5	.338
Likelihood-Quotient	7.305	5	.199
Anzahl der gültigen Fälle	101		
a. 8 Zellen (66.7%) haben eine erwartete Häufigkeit kleiner 5. Die minimale erwartete Häufigkeit ist .28.			

Zusammenhang Bildung – Akzeptanz der Cookies: Pearson-Chi-Quadrat-Test

Kreuztabellen

Zusammenfassung der Fallverarbeitung						
	Fälle					
	Gültig		Fehlend		Gesamt	
	N	Prozent	N	Prozent	N	Prozent
Cookie_Akzeptanz_binär * Ausbildung	101	100.0%	0	0.0%	101	100.0%

Cookie_Akzeptanz_binär * Ausbildung Kreuztabelle								
			Ausbildung					
			Anderes	Maturität	Berufslehre	höhere Berufsbildung	Hochschulabschluss	Gesamt
Cookie_Akzeptanz_binär	Angepasst oder abgelehnt	Anzahl	0	1	2	4	7	14
		Erwartete Anzahl	.1	1.1	3.2	3.6	6.0	14.0
		% von Cookie_Akzeptanz_binär	0.0%	7.1%	14.3%	28.6%	50.0%	100.0%
	Akzeptiert	Anzahl	1	7	21	22	36	87
		Erwartete Anzahl	.9	6.9	19.8	22.4	37.0	87.0

		% von Cookie_Akzeptanz_binär	1.1%	8.0%	24.1%	25.3%	41.4%	100.0%
Gesamt		Anzahl	1	8	23	26	43	101
		Erwartete Anzahl	1.0	8.0	23.0	26.0	43.0	101.0
		% von Cookie_Akzeptanz_binär	1.0%	7.9%	22.8%	25.7%	42.6%	100.0%

Chi-Quadrat-Tests			
	Wert	df	Asymptotische Signifikanz (zweiseitig)
Pearson-Chi-Quadrat	.948[a]	4	.918
Likelihood-Quotient	1.142	4	.888
Zusammenhang linear-mit-linear	.655	1	.418
Anzahl der gültigen Fälle	101		

a. 5 Zellen (50.0%) haben eine erwartete Häufigkeit kleiner 5. Die minimale erwartete Häufigkeit ist .14.

Zusammenhang Geschlecht – Akzeptanz der Cookies: Pearson-Chi-Quadrat-Test

Kreuztabellen

Zusammenfassung der Fallverarbeitung						
	Fälle					
	Gültig		Fehlend		Gesamt	
	N	Prozent	N	Prozent	N	Prozent
Geschlecht * Cookie_Akzeptanz_binär	101	100.0%	0	0.0%	101	100.0%

Geschlecht * Cookie_Akzeptanz_binär Kreuztabelle					
			Cookie_Akzeptanz_binär		
			Angepasst oder abgelehnt	Akzeptiert	Gesamt
Geschlecht	männlich	Anzahl	9	44	53

		Erwartete Anzahl	7.3	45.7	53.0
		% von Geschlecht	17.0%	83.0%	100.0%
	weiblich	Anzahl	5	43	48
		Erwartete Anzahl	6.7	41.3	48.0
		% von Geschlecht	10.4%	89.6%	100.0%
Gesamt		Anzahl	14	87	101
		Erwartete Anzahl	14.0	87.0	101.0
		% von Geschlecht	13.9%	86.1%	100.0%

Chi-Quadrat-Tests

	Wert	df	Asymptotische Signifikanz (zweiseitig)	Exakte Sig. (zweiseitig)	Exakte Sig. (einseitig)
Pearson-Chi-Quadrat	.909[a]	1	.340		
Kontinuitätskorrektur[b]	.442	1	.506		
Likelihood-Quotient	.923	1	.337		
Exakter Test nach Fisher				.398	.254
Anzahl der gültigen Fälle	101				

a. 0 Zellen (.0%) haben eine erwartete Häufigkeit kleiner 5. Die minimale erwartete Häufigkeit ist 6.65.

b. Wird nur für eine 2x2-Tabelle berechnet

Zusammenhang Alter – Akzeptanz der Cookies: Logistische Regression

Logistische Regression

Zusammenfassung der Fallverarbeitung

Ungewichtete Fälle[a]		N	Prozent
Ausgewählte Fälle	Einbezogen in Analyse	101	100.0
	Fehlende Fälle	0	.0
	Gesamt	101	100.0
Nicht ausgewählte Fälle		0	.0

Gesamt	101	100.0
a. Wenn die Gewichtung wirksam ist, finden Sie die Gesamtzahl der Fälle in der Klassifizierungstabelle.		

Codierung abhängiger Variablen	
Ursprünglicher Wert	Interner Wert
Angepasst oder abgelehnt	0
Akzeptiert	1

Block 0: Anfangsblock

Iterationsprotokoll[a,b,c]			
Iteration		-2 Log-Likelihood	Koeffizienten Konstante
Schritt 0	1	83.213	1.446
	2	81.316	1.783
	3	81.293	1.826
	4	81.293	1.827
a. Konstante in das Modell einbezogen.			
b. Anfängliche -2 Log-Likelihood: 81.293			
c. Schätzung beendet bei Iteration Nummer 4, weil die Parameterschätzer sich um weniger als .001 änderten.			

Klassifizierungstabelle[a,b]					
			Vorhergesagt		
			Cookie_Akzeptanz_binär		
	Beobachtet		Angepasst oder abgelehnt	Akzeptiert	Prozentsatz der Richtigen
Schritt 0	Cookie_Akzeptanz_binär	Angepasst oder abgelehnt	0	14	.0
		Akzeptiert	0	87	100.0
	Gesamtprozentsatz				86.1
a. Konstante in das Modell einbezogen.					

b. Der Trennwert lautet .500

Variablen in der Gleichung							
		Regressionskoeffizient B	Standardfehler	Wald	df	Sig.	Exp(B)
Schritt 0	Konstante	1.827	.288	40.247	1	<.001	6.214

Variablen nicht in der Gleichung					
			Wert	df	Sig.
Schritt 0	Variablen	Alter	.002	1	.964
	Gesamtstatistik		.002	1	.964

Block 1: Methode = Einschluß

Iterationsprotokoll[a,b,c,d]				
Iteration		-2 Log-Likelihood	Koeffizienten	
			Konstante	Alter
Schritt 1	1	83.211	1.429	.000
	2	81.314	1.753	.001
	3	81.291	1.792	.001
	4	81.291	1.793	.001
a. Methode: Einschluß				
b. Konstante in das Modell einbezogen.				
c. Anfängliche -2 Log-Likelihood: 81.293				
d. Schätzung beendet bei Iteration Nummer 4, weil die Parameterschätzer sich um weniger als .001 änderten.				

Omnibus-Tests der Modellkoeffizienten				
		Chi-Quadrat	df	Sig.
Schritt 1	Schritt	.002	1	.964
	Block	.002	1	.964
	Modell	.002	1	.964

Modellzusammenfassung			
Schritt	-2 Log-Likelihood	Cox & Snell R-Quadrat	Nagelkerkes R-Quadrat

1	81.291[a]	.000	.000

a. Schätzung beendet bei Iteration Nummer 4, weil die Parameterschätzer sich um weniger als .001 änderten.

Klassifizierungstabelle[a]

			Vorhergesagt		
			Cookie_Akzeptanz_binär		
	Beobachtet		Angepasst oder abgelehnt	Akzeptiert	Prozentsatz der Richtigen
Schritt 1	Cookie_Akzeptanz_binär	Angepasst oder abgelehnt	0	14	.0
		Akzeptiert	0	87	100.0
	Gesamtprozentsatz				86.1

a. Der Trennwert lautet .500

Variablen in der Gleichung

		Regressions-koeffizientB	Standard-fehler	Wald	df	Sig.	Exp(B)	95% Konfidenzintervall für EXP(B)	
								Unterer Wert	Oberer Wert
Schritt 1[a]	Alter	.001	.018	.002	1	.964	1.001	.966	1.037
	Konstante	1.793	.803	4.989	1	.026	6.005		

a. In Schritt 1 eingegebene Variablen: Alter.

7.6 Anhang F - Wahrheitserklärung

«Ich erkläre hiermit, dass ich die vorliegende Arbeit selbständig, ohne Mithilfe Dritter und nur unter Benutzung der angegebenen Quellen verfasst habe und dass ich ohne schriftliche Zustimmung der Studiengangleitung keine Kopien dieser Arbeit an Dritte aushändigen werde.»

Gleichzeitig werden sämtliche Rechte am Werk an die Zürcher Hochschule für angewandte Wissenschaften (ZHAW) abgetreten. Das Recht auf Nennung der Urheberschaft bleibt davon unberührt.

Name der Studierenden
Larissa Mörgeli

Unterschrift der Studierenden