Hochschule
für Wirtschaft und Gesellschaft
Ludwigshafen

Digital Nudging und Nutzerverhalten

Seminararbeit

im Rahmen der Prüfung zum

Bachelor of Science (B.Sc.)

des Studiengangs Internationale Wirtschaftsinformatik (IBAIT)

an der Hochschule für Wirtschaft und Gesellschaft Ludwigshafen

von

Moritz Schley	(633567)
Jana Walcher	(633642)
Paulina Kohlhepp	(633605)
Arkin Cip	(633638)

Abgabedatum:	02.12.2022
Bearbeitungszeitraum:	01.10.2022 - 02.12.2022

Ehrenwörtliche Erklärung

Ich versichere hiermit, dass ich meine Seminararbeit mit dem Thema:

Digital Nudging und Nutzerverhalten

gemäß § 5 der „Studien- und Prüfungsordnung DHBW Technik“ vom 29. September 2017 selbstständig verfasst und keine anderen als die angegebenen Quellen und Hilfsmittel benutzt habe. Die Arbeit wurde bisher keiner anderen Prüfungsbehörde vorgelegt und auch nicht veröffentlicht.

Ich versichere zudem, dass die eingereichte elektronische Fassung mit der gedruckten Fassung übereinstimmt.

Ludwigshafen, den 1. Dezember 2022

Gez. Vorname Nachname
Nachname, Vorname

Inhaltsverzeichnis

Abkürzungsverzeichnis

BGH Bundesgerichtshof

DSA Digital Services Act

DSGVO Datenschutzgrundverordnung

EU Europäische Union

EuGH Europäischer Gerichtshof

HTTP Hypertext Transfer Protocol

Abbildungsverzeichnis

Listings

1 Einführung in die Thematik

yxcyxc

1.1 Definition

yxcyxc

1.2 Ethische Grundlagen

yxcyxcyxc

1.2.1 Autonomität

1.2.2 Transparenz

yxcyxcyxc

1.2.3 Zielrechtfertigung

1.2.4 Weitere Modelle

1.3 Cookie Banner: Manipulativ?

1.3.1 Einleitung in das Beispiel

Internetseiten nutzen zum Anzeigen und Senden von Daten das sogenannte Hypertext Transfer Protocol (HTTP). Bei HTTP handelt es sich um ein sogenanntes “stateless” (zustandsloses) Protokoll, d.h. alle Anfragen und Transaktionen zwischen dem Nutzer und der aufgerufenen Internetseite sind unabhängig voneinander. Dadurch fällt es schwer, Zusammenhänge und Nutzerdaten mehrerer Anfragen mitzusenden und abrufbar zu halten.

Cookies werden eingesetzt, wenn bestimmte Infos zwischen mehreren Anfragen gespeichert werden sollen. Sie sind kleine Dateien, welche von der aufzurufenden Internetseite angefordert und gesendet werden. Die Cookies werden dann vom genutzten Internetbrowser angelegt und verwaltet. Sie sind dabei immer spezisich für die Seite, die sie anfragt und sendet und werden genutzt, um beispielsweise Internetseiten mit Kontofunktionen zu realisieren.[1]

1.3.2 Problemstellung

Obwohl Cookies spezifisch für jede Internetseite sind und ein Verknüpfen von Nutzerdaten über mehrere Internetseiten hinweg nicht möglich sein sollte, wurde durch die Funktionsweise des Internets schnell eine Möglichkeit gefunden, Cookies für mehrere Seiten zu nutzen.

Dabei wird neben der gewünschten Internetseite noch eine weitere Seite geladen, welche den Cookie setzt und anfordert. Wenn dieses System über mehrere Internetseiten hinweg genutzt wird, können die Interessen eines Nutzers nachverfolgt werden. Man spricht hierbei vom “Third Party Cookies”, da das Datensammeln nicht direkt durch den Seitenbetreiber selbst passiert.[2]

[1] Kristol, D. M. (o. D.). „HTTP Cookies: Standards, Privacy, and Politics“. In: *ACM Transactions on Internet Technology* (). URL: http://arxiv.org/pdf/cs/0105018v1, S. 4-6.

[2] Bielova, N. (2017). „Web Tracking Technologies and Protection Mechanisms“. In: *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security*. Hrsg. von Thuraisingham, B. u. a. New York, NY, USA: ACM, S. 2607–2609, S. 2608.

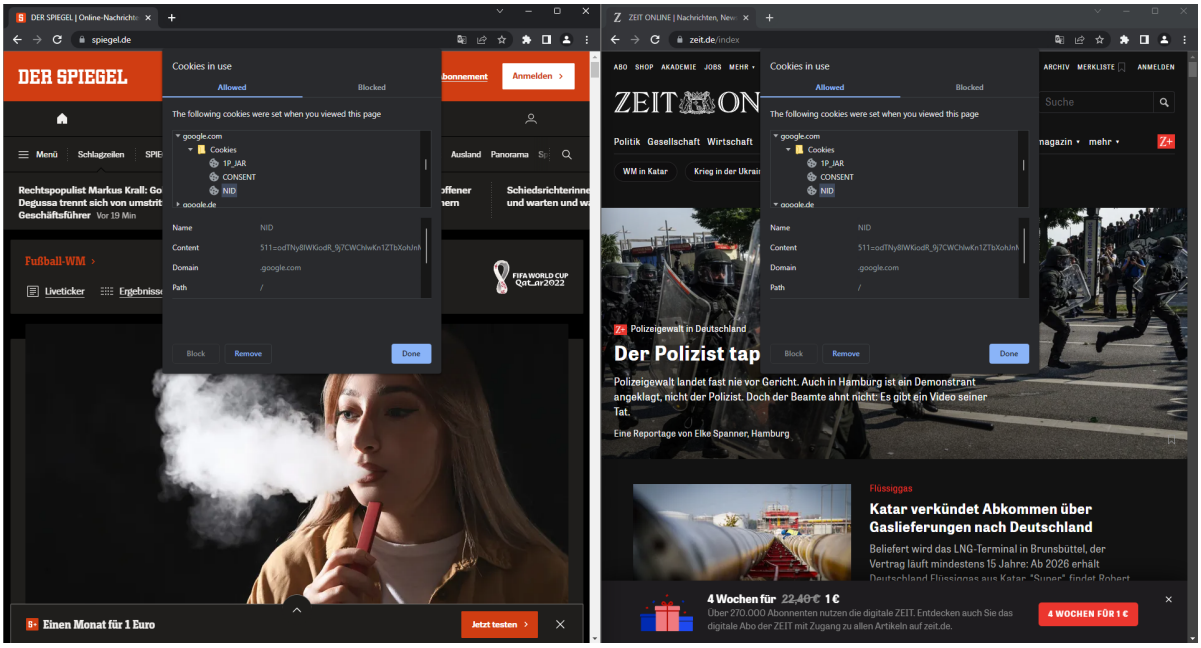

Abbildung 1.1: Ein Third Party Cookie, welcher bei Spiegel und Zeit genutzt wird

Durch Verabschiedung der Datenschutzgrundverordnung (DSGVO) in der Europäische Union (EU) im Jahr 2016[3] gibt es für Cookies in der EU einen rechtlichen Rahmen zur Verwendung jener. Dieser sieht vor, dass lediglich “First Party Cookies”, also Cookies, welche direkt von der aufgerufenen Internetseite erstellt werden, genutzt werden dürfen. Entsprechenden “Third Party Cookies”, welche hauptsächlich zum Sammeln von Nutzerdaten genutzt werden, muss der Nutzer nach der DSGVO erst explizit zustimmen. Die EU erhofft sich davon mehr Transparenz im Bezug auf die Verarbeitung personenbezogener Daten.[4]

[3] Europäische Union (2016). *VERORDNUNG (EU) 2016/679 DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung): Datenschutz-Grundverodnung (DSGVO)*. URL: https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32016R0679&from=DE (Einsichtnahme: 01. 12. 2022).

[4] Europäische Union (2016). *VERORDNUNG (EU) 2016/679 DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung): Datenschutz-Grundverodnung (DSGVO)*. URL: https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32016R0679&from=DE (Einsichtnahme: 01. 12. 2022), S. 84.

Unternehmen ist in vielen Fällen jedoch daran gelegen, möglichst viele “Third Party Cookies” einzubinden. So gibt es ganze Geschäftsmodelle, welche Cookies zu Werbe- und Analysezwecken nutzen und durch das effektive Sammeln und Auswerten von Daten Umsatz generieren.[5] Durch die gegebenen Umstände entwickelte sich so der Trend, dass zur Einwilligung in die Datensammlung ein Nudge genutzt wird, welcher die Entscheidung beeinflussen soll.

1.3.3 Aufbau und Wirkung

Die Zustimmung zu Cookies wird auf Internetseiten meist in Form eines Banners realisiert, welcher den Nudge enthält. Der Cookie Banner fragt dabei den Nutzer, ob das Einsetzen von Drittanbieter Cookies und damit das Sammeln von Daten gestattet ist. Die Gestaltung weicht dabei je nach Plattform stark voneinander ab.

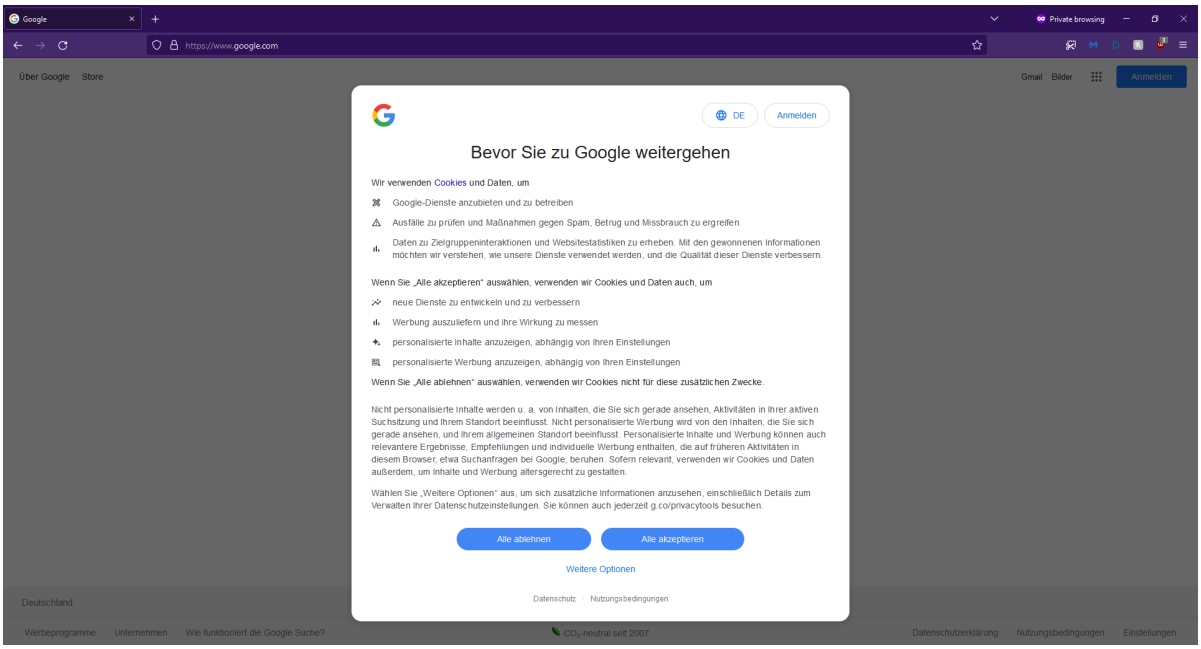

Abbildung 1.2: Cookie Banner auf www.google.com

Beim ersten Aufrufen der Website https://www.google.com wird der Cookiebanner angezeigt. Dabei wird bereits direkt ein Nudge auffällig. Der Banner wird zentral über dem eigentlichen Inhalt des Bildschirms platziert. Der Nutzer, welcher gerade etwas bei

[5] *2012 IEEE Symposium on Security and Privacy* (2012). IEEE, S. 418-420.

Google suchen möchte, muss daher zuerst mit dem Banner interagieren. Google bietet hier einen Knopf “Alles Akzeptieren” und “Alles ablehnen” an. Dennoch wird hier bereits Einfluss auf den Nutzer genommen, da sein Nutzungserlebnis direkt gestört wird und er erst einen der beiden Knöpfe drücken muss, um mit seiner Arbeit fortzufahren.

Auf der Webseite von Facebook (https://www.facebook.com/de) wird neben dem inhaltsverdeckenden Banner ein weiterer Nudge eingesetzt. Die Option “Erforderliche und optionale Cookies erlauben” ist in einem auffälligen Blau markiert, während die Option “Nur erforderliche Cookies erlauben” in einer grauen Farbe gezeigt wird.

Abbildung 1.3: Cookie Banner auf www.facebook.com mit farblich unterschiedlichen Knöpfen

Die farbliche Hervorhebung einer Option erscheint für den Nutzer hierbei wie eine Empfehlung und sticht mehr ins Auge, als der hellgraue Farbton, welcher sehr ähnlich

zum Hintergrund wirkt. Hervorhebung einer gewünschten Option kann nicht nur durch Farbe, sondern auch durch Positionierung und Größe innerhalb des Banners passieren.

Eine weitere Möglichkeit, den Nutzer in seiner Entscheidung zu beeinflussen, stellt das Verlagern der Ablehnen Funktion auf eine Extra Seite dar. Hierbei wird dem Nutzer lediglich eine Option zum Akzeptieren und eine Option zum Ansehen diverser Einstellungen bezüglich des Datenschutzes angeboten.

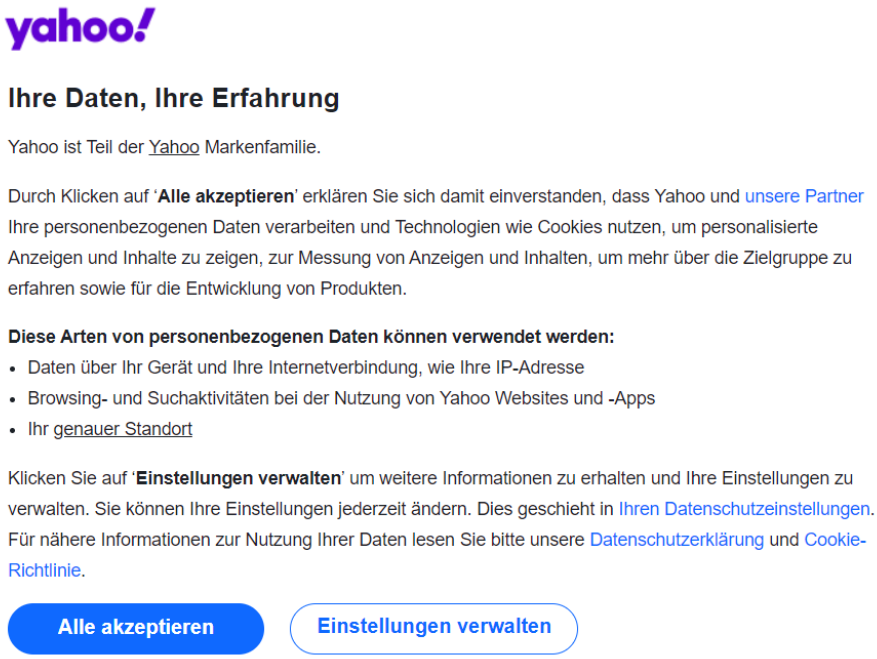

Abbildung 1.4: Cookie Banner auf www.yahoo.de mit Einstellungsknopf

Dieses Verlagern der Ablehnenfunktion auf eine weitere Seite ist besonders effektiv, wenn der Nudge dazu genutzt werden soll, dass Nutzer tendenziell dem Datensammeln zustimmen. Die Zustimmung aller Cookies ist 22 - 23 % wahrscheinlicher, wenn die Ablehnenfunktion nicht direkt im Banner enthalten ist.[6]

[6]Nouwens, M. u. a. (2020). „Dark Patterns after the GDPR: Scraping Consent Pop-ups and Demonstrating their Influence“. In: *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*. Hrsg. von Bernhaupt, R. u. a. New York, NY, USA: ACM, S. 1–13, S. 8.

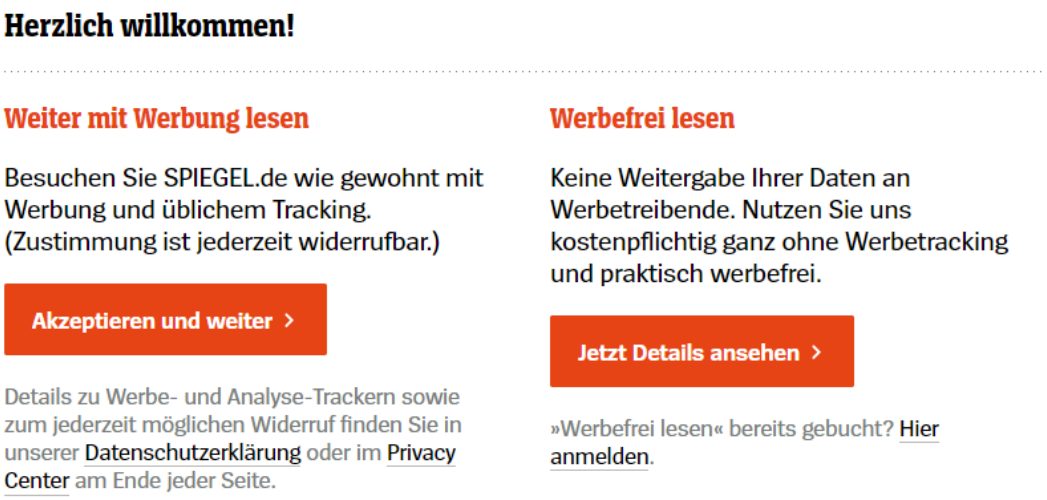

Abbildung 1.5: Cookie Banner auf www.spiegel.de mit Bezahlfunktion

1.3.4 Bewertung anhand der ethischen Grundlagen

Je nach Funktionsweise lässt sich nachweisen, dass die hier gezeigten Beispiele gegen die in Kapitel HIER EINSETZEN verstoßen. Während die Einblendung von Google (siehe Abbildung 1.2) mit den Optionen “Alles Akzeptieren” und “Alles ablehnen” eine transparente und autonome Auswahl der Einstellungen ermöglicht, lässt sich argumentieren, dass die Banner von Facebook (siehe Abbildung 1.3) und Yahoo (siehe 1.4) gegen ethische Grundsätze von digitalen Nudges verstoßen.

In beiden Fällen ist die Transparenz eingeschränkt, da eine Option (Alles akzeptieren) farblich hervorgehoben ist und die Wahl damit nicht mehr neutral ist. Yahoo geht außerdem einen Schritt weiter und bietet gar nicht mehr alle Optionen direkt an (“Alles ablehnen”), sondern versteckt den Inhalt auf einer Einstellungsseite, was nicht nur Transparenz sondern auch Autonomie einschränkt.

Deutsche Zeitungsanbieter nutzen dieses Prinzip und bieten keine Option zum Ablehnen mehr an. Hier wird lediglich vorgeschlagen, die Cookierichtlinien zu akzeptieren oder für ein cookiefreies Modell zu bezahlen.

Hier sind Autonomität und Transparenz noch eingeschränkter, da gar nicht mehr alle Optionen (Cookies ablehnen) angeboten werden. Dem Nutzer wird lediglich angeboten, alle Cookies zu akzeptieren, eine Option alles abzulehnen gibt es nicht mehr.

Abschließend lässt sich sagen, dass die Nutzung von Cookie Bannern bei bekannten Plattformen klar gegen ethische Grundlagen verstößt. Neben den Idealen der Autonomität und Transparenz, verstoßen alle genannten Beispiele auch gegen den Grundsatz der Zielrechtfertigung, da mit dem Aktivieren der Cookies weder soziale noch nutzerfreundliche und lediglich Interessen der Plattform verfolgt werden. Auch rechtlich sind die gezeigten Beispiele bereits kritisiert worden. So verurteilte die französische Datenschutzbehörde Facebook und Google zu hohen Geldstrafen aufgrund von Verstößen gegen die DSGVO im Bezug auf die Implementierung von Cookie-Bannern.[7]

[7] Anna Biselli (2022). *210 Millionen Euro Strafen gegen Google und Facebook*. URL: https://netzpolitik.org/2022/frankreich-210-millionen-euro-strafen-gegen-google-und-facebook/#netzpolitik-pw (Einsichtnahme: 01. 12. 2022).

2 Ethische und rechtliche Probleme bei Digital Nudging

Dieses Kapitel diskutiert Risiken und Probleme, die bei der Verwendung von Digital Nudging auftreten können.

2.1 Helles und dunkles Nudging

Bei der Nutzung von Nudges im digitalen Bereich lässt sich grundsätzlich zwischen hellem und dunklem Nudging unterschieden. Dabei beschreibt helles Nudging einen nach den ethischen Grundlagen "gutenSZweck, während dunkles (dark) Nudging für Zwecke steht, die gegen die ethischen Grundlagen verstoßen.

Wichtig ist dabei, dass Nudging als Instrument in der Diskussion erst einmal neutral ist. Erst durch die Definition eines Anwendungsfalls kann darüber diskutiert werden, ob es sich um einen hellen oder dunklen Nudge handelt.

Dennoch lässt sich in der Wirtschaft abzeichnen, dass Nudging zunehmend für unethische Zwecke verwendet wird. Dafür haben sich die Begriffe “Dark Nudging”, “Sludges” und “Dark Patterns” etabliert.[1] Der Begriff Dark Patterns wurde dabei 2010 erstmals von Brignull definiert und beschreibt Tricks in Webseiten und Apps, die Nutzer:Innen zu Handlungen bewegen, die von ihrer eigentlich gewünschten Handlung abweisen.[2]

[1] Narayanan, A. u. a. (2020). „Dark Patterns: Past, Present, and Future“. In: *Queue* 18.2, S. 67–92, S. 73-74.

[2] Brignull, H. (2010). *Deceptive Design: user interfaces crafted to trick you*. URL: https://www.deceptive.design (Einsichtnahme: 01. 12. 2022).

Wissenschaftler haben herausgefunden, dass Dark Patterns in über 1200 Shopping Seiten[3] und in mehr als 95% von beliebten Android Apps[4] implementiert sind. Daran lässt sich erkennen, dass Dark Nudging sehr in den Alltag von Nutzerinnen und Nutzern eingreift und kein Randphänomen ist.

Thaler, der wie in Kapitel (HIER EINSETZEN) die Theorie hinter Nudging eingeführt hat, distanziert sich mittlerweile öffentlich von der Dark Patterns Nutzung seiner Idee. Er nennt unethische Nudges “Sludges”. Seiner Ansicht nach sollten Nudges nur genutzt werden, um die Umgebung, in der Menschen Enrscheidungen treffen angenehmer zu gestalten. Dies ermögliche selbstbewusstere Entscheidungen. Dark Pattern beschreibt er als "nudging for evil".[5]

2.2 Rechtliche Situation

Die Präsenz des Themas im alltäglichen Gebrauch lässt auch die Gesetzgebung in Deutschland und der EU auf das Thema aufmerksam werden. Auch wenn es bisher keine einheitliche Regelung bezüglich Digital Nudging und Dark Patterns gibt, so sind in Einzelfällen (wie bspw. in HIER KAPITEL EINSETZEN) bereits rechtliche Grundlagen zur Nutzung von Nudges gesetzt worden.

Der Gewinnspielbetreiber "Planet49"hatte bei seinem Cookie Banner standardmäßig alle Cookies mit Ankreuzkästchen aktiviert. Zum Ablehnen der Datensammlung war es notwendig, die Häkchen nach und nach anzuklicken. Der Bundesverband der deutschen Verbraucherzentralen und Verbraucherverbände hat gegen diese Implementierung geklagt. In einem Urteil des Europäischer Gerichtshof (EuGH), welches später durch den deutschen Bundesgerichtshof (BGH) bestätigt wurde, wird erläutert, dass eine wirksame Einwilligung nicht durch vorausgewählte Einstellungen erfolgen könne. Außerdem seien zu einer vollständigen Einwilligung weitere Informationen

[3] Mathur, A. u. a. (2019). „Dark Patterns at Scale“. In: *Proceedings of the ACM on Human-Computer Interaction* 3.CSCW, S. 1–32, S. 2.

[4] Di Geronimo, L. u. a. (2020). „UI Dark Patterns and Where to Find Them“. In: *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*. Hrsg. von Bernhaupt, R. u. a. New York, NY, USA: ACM, S. 1–14, S. 5.

[5] Thaler, R. H. (2018). „Nudge, not sludge“. In: *Science (New York, N.Y.)* 361.6401, S. 431.

notwendig, wie z.B. die Funktionsdauer der Cookies oder mit welchen Drittanbietern sie geteilt werden.[6]

Aktuell befasst sich die EU im Rahmen des Digital Services Act (DSA) mit Dark Patterns. So plant die EU, Dark Patterns weitreichend zu verbieten. “Anbietern von Online-Plattformen sollte es [...] untersagt sein, die Nutzer in die Irre zu führen oder zu etwas zu verleiten und die Autonomie, die Entscheidungsfreiheit oder die Auswahlmöglichkeiten der Nutzer durch den Aufbau, die Gestaltung oder die Funktionen einer Online-Schnittstelle oder eines Teils davon zu verzerren oder zu beeinträchtigen.”[7] Damit gibt es erstmalig eine Rechtsgrundlage zur allgemeinen Benutzung von Nudes im digitalen Raum. Dennoch gibt es Bedenken, dass die Forderungen des DSA nicht weitreichend genug seinen, etwa weil sich der die Regelungen nur auf “Online-Plattformen” beziehen, worunter nicht alle Internetseiten fallen.[8] Es bleibt abzuwarten, wie effektiv die Regelungen des DSA sind und ob Plattformbetreiber ihre Inhalte nach Inkrafttreten der Verordnung in den Mitgliedsstaaten anpassen.

[6] Hartung, J. und Schwarze, P. (2020). *„Planet49“-Urteil des BGH: Keine wirksame Einwilligung zu Cookies durch voreingestelltes Opt-In*. URL: https://www.oppenhoff.eu/de/news/detail/planet49-urteil-des-bgh-keine-wirksame-einwilligung-zu-cookies-durch-voreingestelltes-opt-in/ (Einsichtnahme: 01. 12. 2022).

[7] Europäische Union (2022). *VERORDNUNG (EU) 2022/2065 DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 19. Oktober 2022 über einen Binnenmarkt für digitale Dienste und zur Änderung der Richtlinie 2000/31/EG (Gesetz über digitale Dienste): Digital Services Act (DSA)*. URL: https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32022R2065&from=en (Einsichtnahme: 01. 12. 2022), S. 18.

[8] King, J. und MacKinnon, E. (2022). *Do the DSA and DMA Have What It Takes to Take on Dark Patterns?* URL: https://techpolicy.press/do-the-dsa-and-dma-have-what-it-takes-to-take-on-dark-patterns/ (Einsichtnahme: 01. 12. 2022).

Literaturverzeichnis

2012 IEEE Symposium on Security and Privacy (2012). IEEE.

Anna Biselli (2022). *210 Millionen Euro Strafen gegen Google und Facebook*. URL: https://netzpolitik.org/2022/frankreich-210-millionen-euro-strafen-gegen-google-und-facebook/#netzpolitik-pw (Einsichtnahme: 01. 12. 2022).

Bielova, N. (2017). „Web Tracking Technologies and Protection Mechanisms“. In: *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security*. Hrsg. von Thuraisingham, B. u. a. New York, NY, USA: ACM, S. 2607–2609.

Brignull, H. (2010). *Deceptive Design: user interfaces crafted to trick you*. URL: https://www.deceptive.design (Einsichtnahme: 01. 12. 2022).

Di Geronimo, L. u. a. (2020). „UI Dark Patterns and Where to Find Them“. In: *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*. Hrsg. von Bernhaupt, R. u. a. New York, NY, USA: ACM, S. 1–14.

Europäische Union (2016). *VERORDNUNG (EU) 2016/679 DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung): Datenschutz-Grundverodnung (DSGVO)*. URL: https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32016R0679&from=DE (Einsichtnahme: 01. 12. 2022).

– (2022). *VERORDNUNG (EU) 2022/2065 DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 19. Oktober 2022 über einen Binnenmarkt für digitale Dienste und zur Änderung der Richtlinie 2000/31/EG (Gesetz über digitale Dienste): Digital Services Act (DSA)*. URL: https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32022R2065&from=en (Einsichtnahme: 01. 12. 2022).

Hartung, J./ P. Schwarze (2020). *„Planet49“-Urteil des BGH: Keine wirksame Einwilligung zu Cookies durch voreingestelltes Opt-In*. URL: https://www.oppenhoff.eu/de/news/detail/planet49-urteil-des-bgh-keine-wirksame-einwilligung-zu-cookies-durch-voreingestelltes-opt-in/ (Einsichtnahme: 01. 12. 2022).

King, J./ E. MacKinnon (2022). *Do the DSA and DMA Have What It Takes to Take on Dark Patterns?* URL: https://techpolicy.press/do-the-dsa-and-dma-have-what-it-takes-to-take-on-dark-patterns/ (Einsichtnahme: 01. 12. 2022).

Kristol, D. M. (o. D.). „HTTP Cookies: Standards, Privacy, and Politics“. In: *ACM Transactions on Internet Technology* (). URL: http://arxiv.org/pdf/cs/0105018v1.

Mathur, A. u. a. (2019). „Dark Patterns at Scale“. In: *Proceedings of the ACM on Human-Computer Interaction* 3.CSCW, S. 1–32.

Narayanan, A. u. a. (2020). „Dark Patterns: Past, Present, and Future“. In: *Queue* 18.2, S. 67–92.

Nouwens, M. u. a. (2020). „Dark Patterns after the GDPR: Scraping Consent Pop-ups and Demonstrating their Influence“. In: *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*. Hrsg. von Bernhaupt, R. u. a. New York, NY, USA: ACM, S. 1–13.

Thaler, R. H. (2018). „Nudge, not sludge“. In: *Science (New York, N.Y.)* 361.6401, S. 431.