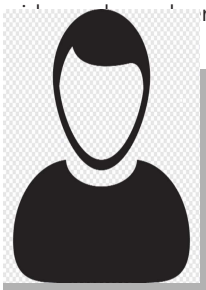
Dark Patterns – eine interdisziplinäre Analyse

Prof. Dr. Michael Gertz, Prof. Dr. Mario Martini, Paul Seeliger,
Dr. Christina Timko

Der Trendbegriff „Dark Patterns“ hat Konjunktur. Er ist ebenso omnipräsent wie interpretationsoffen. Designmuster, die den Nutzer in eine verbraucherschädigende Richtung lenken sollen, stellen Wissenschaft, Regulierungsbehörden und den Gesetzgeber gleichermaßen vor besondere Herausforderungen. Immer klarer wird: Um Dark Patterns in all ihren Facetten zu beleuchten und Gefahren für Verbraucher [illegible]n, bedarf es eines interdisziplinären Schulterschlusses der Verhaltensökonomie, Rechtswissenschaft und Informatik.



Prof. Dr. Michael Gertz: Michael Gertz ist Professor am Institut für Informatik der Universität Heidelberg.Prof. Dr. Mario Martini: Mario Martini ist Lehrstuhlinhaber an der DUV Speyer und Leiter des Programmbereichs Transformation des Staates in Zeiten der Digitalisierung am Deutschen Forschungsinstitut für öffentliche Verwaltung (FÖV).Paul Seeliger: Paul Seeliger ist juristischer Forschungsreferent am FÖV und Koordinator des Dark-Patterns-Detection-Projekts (www.dapde.de), welches das BMUV fördert.Dr. Christina Timko: Christina Timko ist promovierte Verhaltensökonomin am Lehrstuhl für Makroökonomik der Ruhr-Universität Bochum.

I. Einführung

Fragt man Passanten auf der Straße nach Dark Patterns, zucken viele nur mit den Schultern. Das dahinterstehende Phänomen kennt jedoch nahezu jeder. Insbesondere auf Cookie-Bannern[1] begegnen uns Dark Patterns im digitalen Alltag häufig.[2] Diese legen es Nutzern beispielsweise nahe, Cookies pauschal zu akzeptieren, statt sie über zeitraubende Klick-Folgen im Browser abzulehnen.[3] Designer verwenden insbesondere Farbschemata oder Größenverhältnisse, die die Zustimmung weniger aufwendig als ihre Alternative erscheinen lassen; vereinzelt lassen die Cookie-Banner es auf erster Ebene gar nicht zu, die Einwilligung zu verweigern (s. Abbildung 1).[4]

Abbildung 1: Ein Misdirection-Pattern, das eine Entscheidungsoption („Alle akzeptieren“) deutlich hervorhebt.[5]

Den Topos „Dark Patterns“ hat 2010 Harry Brignull, ein Spezialist für das Design von User Interfaces, aus Ärger über täuschende, manipulierende oder umständlich zu bedienende digitale Oberflächen in die Diskussion eingeführt.[6] Mittlerweile findet sich für das Phänomen eine Vielzahl ähnlicher begrifflicher Umschreibungen, wie beispielsweise „Deceptive Design“ oder „Dark Strategies“.[7] Eine einheitliche und universell operationalisierbare Definition hat sich bis dato nicht durchgesetzt. Das liegt auch an den unterschiedlichen Perspektiven der Disziplinen, die auf verhaltensbeeinflussendes Design blicken: Die rechtliche Regulierung datenschutzrelevanter Dark Patterns rückt andere Aspekte in den Blick als die verhaltensökonomische Analyse von Nutzerinteressen im Onlinehandel – ebenso wie die Informatik sich auf bereichsspezifisch ausgeformte Phänomenbeschreibungen fokussiert, um ausführbare Algorithmen zu entwickeln, die manipulative Elemente in praxi erkennen. Umso wichtiger ist es daher, eben diese divergierenden wissenschaftlichen Blickwinkel zusammenzuführen.[8]

Obgleich die konkreten Fragestellungen in den jeweiligen Disziplinen variieren mögen, lassen sich Dark Patterns doch auf eine Essenz verdichten: Ihre Verwender sind in der Regel große Anbieter von Webseiten, Plattformen oder Apps, die

1 Der EuGH hat mit seinem Urteil in der Sache Planet49 vom 1.10.2019 klargestellt, dass jedenfalls sog. „Opt-out“- Lösungen bei Cookie-Bannern, also Anzeigen, bei denen der Betreiber das Häkchen für die Einwilligung in die Cookie-Setzung und die daraus folgende Datenverarbeitung bereits gesetzt hat, keine wirksame Einwilligung im Sinne der DSGVO sind, da der Wortlaut ein aktives Einwilligen und kein passives „Hinnehmen“ voraussetze. EuGH Urt. v. 1.10.2019 – C-673/17, MMR 2019, 732 (735).

2 Santos/Rossi/Chamorro/Bongard-Blanchy/Abu-Salma, Proceedings of the 20th Workshop on Workshop on Privacy in the Electronic Society, 2021, S. 187.

3 Änderungen ergeben sich langsam; so nutzt Alphabet (vormals Google) mittlerweile den „Alle Ablehnen“-Button; vgl. CNIL, Cookies: the CNIL fines GOOGLE a total of 150 million euros, 6.1.2022, https://www.cnil.fr/en/cookies-cnil-fines-google-total-150-million-euros-and-facebook-60-million-euros-non-compliance (letzter Zugriff am 10.1.2023).

4 Siehe dazu beispielsweise die Analyse von 2957 Cookie-Bannern bei Kramme/Kamke/Hausner, Dark patterns and cookie banners: How design influences our consent behavior, 25.3.2022, https://blog.ai-laws.org/dark-patterns-and-cookie-banners-how-design-influences-our-consent-behavior/ (letzter Zugriff am 17.10.2022).

5 Die Grafiken dieses Beitrags sind abrufbar unter https://dapde.de/de/dark-patterns/arten-und-beispiele/ und nach der CC BY 4.0-Lizenz verwendbar.

6 Siehe auch: Types of deceptive design, https://www.deceptive.design/ (letzter Zugriff am 1.8.2022), mit Beispielen zu Dark Patterns.

7 Etwa bei Bösch/Erb/Kargl/Kopp/Pfattheicher, Proceedings on Privacy Enhancing Technologies, 2016, S. 237 (239 ff.). Die unterschiedlichen Benennungen beruhen ua darauf, dass einige Stimmen den Begriff „Dark Patterns“ aus postkolonialer Perspektive kritisch sehen; vgl. Sinders, What’s In a Name? Unpacking Dark Patterns versus Deceptive Design, 18.6.2022, https://medium.com/@carolinesinders/whats-in-a-name-unpacking-dark-patterns-versus-deceptive-design-e96068627ec4 (letzter Zugriff am 19.8.2022). Da sich allerdings gerade erst eine wissenschaftliche Diskussion unter dem Oberbegriff „Dark Patterns“ konsolidiert hat und diverse Gesetzgebungsverfahren ihn nutzen, greift auch dieser Text darauf zurück.

8 Daraus lassen sich wiederum disziplinübergreifende Anstöße ableiten. Ob digitale Gestaltungen etwa lauterkeitsrechtlich problematisch sind oder sein sollten, lässt sich beispielsweise leichter beantworten, wenn automatisierte Erhebungen ihre Verbreitung erfasst und verhaltensökonomische Studien die Anfälligkeit von Verbrauchern ausgeleuchtet haben.

komplexe Online-Umgebungen kreieren.[9] Die Akteure setzen die digitale Architektur nicht nur ein, um eine möglichst angenehme User Experience zu schaffen. Sie nutzen sie vielmehr auch, um ihre eigenen wirtschaftlichen Interessen auf Kosten der Nutzerpräferenzen einseitig durchzusetzen und missbrauchen so ihre Gestaltungsmacht – insbesondere indem sie Besonderheiten oder Verzerrungen der menschlichen Entscheidungsfindung ansprechen, also manipulieren, Druck ausüben oder täuschen. Dies geschieht absichtlich oder ungewollt und meistens, weil die Verwender erfolgreiche Designtrends nachahmen.[10] Verleiten Oberflächengestaltungen eine kritische Zahl an Nutzern zu einem tendenziell verbraucherschädigenden Verhalten und nutzen dabei die Gestaltungsmacht über Benutzeroberflächen einseitig im Interesse ihrer Verwender aus, zeigen sich darin alle typischen Merkmale des Phänomens „Dark Patterns".[11]

Das Macht(un-)gleichgewicht zwischen Unternehmern und Verbrauchern ist, ebenso wie missbräuchliches Verhalten, kein neues Phänomen des Verbraucherschutzes. Dark Patterns (und weitere Methoden digitaler Beeinflussung) sind aber trotzdem nicht bloß alter Wein in neuen Schläuchen. Denn sie wirken in der Regel deutlich subtiler auf die Entscheidungsfreiheit des Individuums ein als der (nicht nur sprichwörtliche) Fuß in der sich schließenden Wohnungstür. Obgleich Dark Patterns isoliert betrachtet keine unüberwindbaren Barrieren aufbauen, ist ihr manipulatives Potenzial besonders hoch, weil sie häufig unterhalb der Wahrnehmungsschwelle wirken und ein Großteil der Verbraucher im schnelllebigen Gewirr des digitalen Alltags täglich mit ihnen konfrontiert ist.[12]

II. Verhaltensökonomische Aspekte

Manipulierende Designmuster nutzen oft Unzulänglichkeiten des menschlichen Entscheidungsverhaltens aus oder verstärken diese Schwächen sogar, beispielsweise indem sie Zeitdruck aufbauen, sozialen Wettbewerb induzieren oder Nachrichten einblenden, die eine faktisch nicht vorhandene Knappheit suggerieren (s. Abbildung 2). Das verzerrt die Wahrnehmung und Wertschätzung der Kunden für Produkte bzw. Dienstleistungen. Die Verzerrungen schlagen in monetäre oder nicht erfasste und nicht wahrgenommene Kosten und Risiken um.

Andere Kategorien manipulativen Designs zielen darauf ab, Nutzer an digitale Anwendungen zu gewöhnen oder es ihnen zu erschweren, sich von Diensten oder Abonnements abzumelden. Die Anbieter setzen dabei gezielt Belohnungssysteme (zB Treuepunkte oder Selbst-Tracking), bindungsstärkende Handlungen in sozialen Netzwerken (zB das Teilen, den Like-Button, soziale Vergleiche, Wettbewerb) oder ablenkende Push-Nachrichten ein, um die neuen Gewohnheiten zu verfestigen. Bei der Verhaltensbeeinflussung machen die Anbieter sich gerne auch die Steuerungskraft des Default-Effekts zunutze. Denn Nutzer ändern Voreinstellungen des Anbieters typischerweise nicht ab.[13]

Abbildung 2: Ein Countdown-Dark Pattern, das Nutzer unter Entscheidungsdruck setzt.

Auf welchen Geschäftsmodellen ihre digitale Umwelt beruht, machen Anbieter typischerweise nicht öffentlich. Sie profitieren davon, dass es vielen Verbrauchern nicht gelingt, die inneren Zusammenhänge und Mechanismen der steuernden Muster zu durchschauen, die hinter Dark Patterns stecken. So orientiert sich das Verhaltensdesign der Unternehmen konzeptionell häufig nicht am Leitbild des Nutzers als mündigem Kunden mit Bedürfnissen und Anforderungen, sondern am „abgestumpften Nutzer" (Dull User). Designer und Softwareentwickler bezeichnen Dull User auch als „dümmste anzunehmende Nutzer".

In einer Umwelt, die den Nutzern Entscheidungen abnimmt und abweichendes Verhalten – auch durch sozialen Druck, Netzwerkeffekte und Skalieren[14] – erschwert, handelt der Dull User typischerweise so, wie Anbieter es von ihm erwarten: Er erkennt Dark Patterns nicht oder hört jedenfalls auf, sich gegen sie zu wehren. Denn dies ringt ihm häufig einen individuell unverhältnismäßig hohen Aufwand ab: Er müsste etwa

9 Combs/Brown, Digital behavioral design, 2018, S. 15.

10 Timko/Schmidt/Niederstadt/Roos/Hoeren/Pinelli, Künstliche Intelligenz – Ethik und Recht 2022, 363.

11 Martini/Drews/Seeliger/Weinzierl ZfDR 2021, 47 (53). Vgl. auch die Definitionen bei: Bogenstahl, Dark Patterns, November 2019, doi:10.5445/IR/1000133932, S. 1: „die deren eigentlicher Intention zuwiderlaufen", „Nachteile oder negative Konsequenzen"; https://www.deceptive.design/ (letzter Zugriff am 1.8.2022): „things that you didn't mean to"; Forbrukerrådet, Deceived by Design, 27.6.2018, https://fil.forbrukerradet.no/wp-content/uploads/2018/06/2018-06-27-deceived-by-design-final.pdf (letzter Zugriff am 17.10.2022) S. 7: „not in their interest"; Gray/Kou/Battles/Hoggatt/Toombs, Proceedings of the 2018 CHI, Paper 534, S. 1 (1): „not in the users best interest"; Luguri/Strahilevitz Journal of Legal Analysis 13 (1) 2021, 43 (61): „things they might not otherwise do".

12 Europäische Kommission, Behavioural study on unfair commercial practices in the digital environment, April 2022, doi:10.2838/469916, S. 85 ff.; Mathur/Acar/Friedman/Lucherini/Mayer/Chetty/Narayanan Proceedings of the ACM on Human-Computer Interaction 2019, Article No. 81, S. 1.

13 Dazu bspw. Cronqvist/Thaler American Economic Review 94 (2) 2004, 424.

14 Skalieren beschreibt die Fähigkeit, zusätzliche Einheiten eines Verbrauchsguts herzustellen, ohne größere zusätzliche Investitionen zu tätigen. Beispielsweise sind digitale Dienstleistungen leicht millionenfach replizierbar. Damit ist Skalierung eine bedeutende Eigenschaft von Geschäftsmodellen, die das Ziel verfolgen, schnelles Wachstum zu erzielen.

auf digitale Anwendungen verzichten, Kleingedrucktes lesen, auf Webseiten behutsamer klicken, zusätzliche Medienkompetenz, inklusive Kenntnisse des Verhaltensdesigns und missbräuchlicher Muster, aufbauen, zugrunde liegende Geschäftsmodelle hinterfragen u. v. m.

Um einseitigen Geschäftsinteressen und ungewollter Personalisierung entgegenzuwirken, wehren sich einige Verbraucher mit falschen Identitäten und Datenangaben[15] oder nutzen Verschleierungssoftware, um das eigene Online-Verhalten (zB Such- und Klickverhalten)[16] und die Online-Meinung[17] zu tarnen. Die Eigeninitiative der Verbraucher allein wird indes nicht ausreichen, um entsprechende Geschäftspraktiken einzudämmen. Oftmals sind manipulierende Designmuster nämlich überflutend und komplex, so dass sie individuelle Anpassungen und Selbstschutzmaßnahmen überlisten. In anderen Fällen ist das Verhaltensdesign so stark, dass es Verbraucher „hookt", ihre Gewohnheiten umformt und schließlich zu suchtartigem Verhalten führt.[18] Das Tückische an Sucht ist, dass sie die Wahrnehmung trübt.[19] Facebook-Experimente machten das beispielhaft deutlich: Sie zeigten, dass die Wertschätzung für das soziale Netzwerk massiv sank, nachdem Verbraucher es einige Wochen lang abgeschaltet hatten.[20]

Teilweise sind digitale Dienste überdies unverzichtbar geworden, so dass eine strikte Vermeidungsstrategie keine praktikable Antwort ist. Insbesondere Verbraucher, die nicht über das Wissen verfügen, um eigenhändig technische Lösungen zu implementieren, sind somit umso mehr auch auf wohlwollenden systematischen Verbraucherschutz angewiesen.

Softwareentwicklern kommt in diesem Schutzkonzept eine wichtige Rolle zu. Auf dem unzureichend regulierten Feld digitaler Designmuster sehen sie sich häufig in der Zwickmühle zwischen ihrem inneren moralischen Kompass und dem wettbewerblichen Trenddruck.[21] Letzterer stiftet sie dazu an, die Moral bis an die Grenzen des rechtlich Zulässigen zu dehnen. Einige Softwareentwickler berichten, dass sie fragwürdige Projekte verlassen und damit individuell die Kosten für ein systematisches gesellschaftliches Problem tragen.[22] Diese Flucht beraubt sie jedoch ihrer Gestaltungsmacht, so dass die Moral im schlimmsten Fall von Generation zu Generation erodiert. Aus gesamtgesellschaftlicher Sicht wäre es umgekehrt wünschenswert, wenn Softwareentwickler an der Entwicklung von Legal-Tech-Lösungen mitwirkten, die Dark Patterns und ihre Risiken schon in der Designphase klar benennen und im Interesse der Öffentlichkeit entlarven.

III. Juristische Aspekte

Der nationale Gesetzgeber adressiert Dark Patterns bislang nicht ausdrücklich. Zahlreiche manipulierende Designmuster unterliegen in der Sache aber bereits beschränkenden gesetzlichen Regelungen.[23]

1. Bestehende Regulierung von Dark Patterns

Insbesondere das *Verbrauchervertragsrecht* hält (jedenfalls mittelbar) einige Schutzmechanismen gegen Dark Patterns vor, etwa Widerrufsrechte (siehe v.a. § 355 BGB) oder Informationspflichten.[24] Durch Hinweispflichten des Anbieters unterbindet der Gesetzgeber beispielsweise sog. Hidden Cost-Patterns, die Nutzer erst in einem späteren Bestellschritt über zusätzliche Gebühren oder Kosten informieren (und damit den Sunk-Cost-Effekt[25] ausnutzen): Der Unternehmer muss bei Verbrauchergeschäften die Gesamtkosten bereits in der Werbephase ausweisen (§ 1 Abs. 1 und 3, § 2 PAngV). Auch Anfechtungsrechte wegen Täuschung (§ 123 Abs. 1 Alt. 1 BGB) und Irrtum sowie der Anspruch auf Rückabwicklung des Vertrages wegen Verletzung vorvertraglicher Wahrheits- und Aufklärungspflichten (§§ 280 Abs. 1, 311 Abs. 2, 241 Abs. 2 BGB) setzen Dark Patterns normativ Grenzen.

Mit seinem etwas anders gelagerten Zielfokus, die Redlichkeit des Wettbewerbs zu schützen, tritt das *Wettbewerbsrecht* ebenfalls vielen Gestaltungsformen von Dark Patterns entgegen. Vor allem solche geschäftlichen Handlungen, die aggressiv (§ 4a UWG), irreführend (§§ 5, 5a UWG) oder belästigend (§ 7 UWG) sind, setzt das UWG Grenzen, indem es sie als unlauter einstuft. An mehreren Stellen verbietet es ausdrücklich geschäftliche Handlungen, die den Betroffenen zu Entscheidungen veranlassen, welche er „andernfalls nicht getroffen hätte" (§ 4a Abs. 1 Satz 1, § 5 Abs. 1 UWG) – und lässt schon durch diese Nähe zur gängigen Definition von Dark Patterns die Ähnlichkeit der gesetzlichen Zielrichtung aufscheinen. Unter solche verbotenen geschäftlichen Handlungen können etwa Dark Patterns fallen, die den Nutzer unter Druck setzen (Nagging Patterns) oder ihn faktisch zu ungewollten Klicks nötigen (Obstruction Patterns).

Auch die „Schwarze Liste" des Anhangs zu § 3 Abs. 3 UWG erfasst einige Fälle von Dark Patterns, etwa spezifische Formen von Lockangeboten (Nr. 6), unwahre Angaben über die begrenzte zeitliche Verfügbarkeit von Waren oder Dienstleistungen (Nr. 7) sowie gefälschte oder als authentisch präsentierte, aber ungeprüfte Verbraucherbewertungen (Nr. 23b, 23c – Social Proof-Patterns; s. Abbildung 3).

15 Beispielsweise durch Nutzung von Verschleierungsdienstleistungen von https://temp-mail.org/de/ oder https://emailfake.com/, meistens im Kontext von sozialen Medien.
16 Brunton/Nissenbaum, Obfuscation – A User's. Guide for Privacy and Protest, 2016.
17 Tang/Ghorbani/Chorus The Journal of Mathematical Sociology 2021, 315.
18 Eyal/Hoover, Hooked: How to Build Habit-Forming Products, 2014.
19 Allcott/Gentzkow/Song American Economic Review 112 (7) 2022, 2424.
20 Allcott/Braghieri/Eichmeyer/Gentzkow American Economic Review 110 (3) 2020, 629.
21 Timko/Schmidt/Niederstadt/Roos/Hoeren/Pinelli, Künstliche Intelligenz – Ethik und Recht 2022, 363 (379).
22 Timko/Schmidt/Niederstadt/Roos/Hoeren/Pinelli, Künstliche Intelligenz – Ethik und Recht 2022, 363 (383).
23 Siehe dazu ausführlich Martini/Drews/Seeliger/Weinzierl ZfDR 2021, 47 (53 ff.).
24 Dazu und im Folgenden auch Denga ZfDR 2022, 229 (245 ff.).
25 Grundlegend Arkes/Blumer Organizational Behavior and Human Decision Processes 1985, 124.

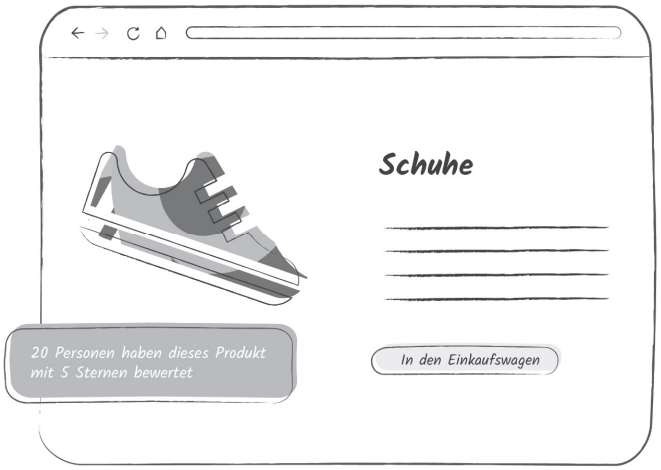


Abbildung 3: (Angebliche) Nutzerbewertungen können Social Proof-Dark Patterns darstellen und unter Nr. 23b, 23c Anh. Zu § 3 Abs. 3 UWG fallen.

Ursprünglich sollten die wettbewerbsrechtlichen Generalklauseln nicht-digitalen, verbraucherschädigenden Praktiken Einhalt gebieten. Sie finden grundsätzlich aber gleichermaßen auf Ausprägungen von Dark Patterns Anwendung und schieben ihrem Einsatz im digitalen geschäftlichen Verkehr gegenüber Verbrauchern abseits der partiellen Einzelfallverbote zumindest teilweise einen Riegel vor.

Aber auch im Wettbewerbsrecht fordern Dark Patterns kraft ihres spezifischen Zuschnitts die Rechtsordnung besonders heraus.[26] Das illustrieren paradigmatisch Fallgestaltungen, in denen ein Anbieter ein Scarcity-Pattern nutzt und Meldungen (wie „Sie sehen unsere letzten Angebote“) einblendet, sobald sich Webseiten-Besucher ein Produkt länger als 15 Sekunden anschauen. Dieser Hinweis kann (insbesondere in Kombination mit weiteren Hinweisen) den unterbewussten Impuls auslösen, eine schnelle Kaufentscheidung treffen zu müssen.[27] Denn dass der Anbieter diese Nachricht nicht individualisiert, sondern pauschal anzeigen lässt, kann der Außenstehende nicht erkennen, sondern fasst sie (in der Regel) als individuellen Hinweis auf. Rechtlich kann diese Aussage als irreführende Angabe iSd § 5 Abs. 1 UWG einzustufen sein. Ob das der Fall ist, bestimmt sich danach, wie ein durchschnittlicher Verbraucher diese Knappheitsmitteilung interpretiert (§ 3 Abs. 4 Satz 1 UWG).[28] Die missbräuchliche Wirkung dieser Designgestaltung liegt jedoch allenfalls teilweise darin begründet, dass Verbraucher sich auf der Grundlage falscher Informationen für oder gegen den Kauf eines Produktes entscheiden. Ausschlaggebend ist vielmehr, dass der Abwägungsprozess wegen einer Drucksituation von vornherein unterbleibt. Im Ergebnis treffen Verbraucher in beiden Fällen keine informierte Entscheidung und sind daher in besonderem Maße schutzwürdig.

Da manche Typen von Dark Patterns gleichsam durch das normative Rost des nationalen Rechts fallen, erfasst es allen bestehenden Regelungen zum Trotz (ebenso wie die Rechtssysteme anderer EU-Mitgliedstaaten) Dark Patterns bisher in Summe nicht systematisch, sondern eher einzelfallbezogen. Es verbleiben weiterhin Regelungslücken.

2. Legislative Bestrebungen der Europäischen Union

Mit Blick auf die bestehenden Sollbruchstellen im Recht der Mitgliedstaaten geraten Dark Patterns zunehmend in den regulatorischen Fokus der Europäischen Union: Sowohl der Entwurf für die *KI-Verordnung* (KI-VO)[29] als auch der *Digital Services Act* (DSA)[30] und der *Digital Markets Act* (DMA)[31] halten Regelungen vor, die manipulierendem Design Schranken setzen sollen.

Der *DSA* verpflichtet Anbieter von Online-Plattformen dazu, ihre Nutzer nicht via Online-Schnittstellen zu täuschen, zu manipulieren oder anderweitig in der Entscheidungsfreiheit einzuschränken (Art. 25 Abs. 1 DSA). Er nimmt (implizit sowie in ErwGr. 67 DSA explizit) auch Dark Patterns ins Visier.

Bei einem allgemeinen Verbot lässt es der Unionsgesetzgeber nicht bewenden. Er adressiert vielmehr insbesondere ausdrücklich Nagging Dark Patterns, also solche Gestaltungsmuster, die Nutzer wiederholt auffordern, dem Anbieter Rechte einzuräumen – ferner Gestaltungen, die es umständlicher machen, sich bei Diensten abzumelden als sich bei diesen anzumelden (sog. Roach Motel), sowie Formen der Interface Interference, die einzelne Entscheidungsalternativen hervorhebt (Art. 25 Abs. 3 lit. a-c, ErwGr. 67 S. 4 und 5 DSA).

Die Aufzählung des Art. 25 Abs. 3 DSA verleiht dem generellen Verbot des Abs. 1 zwar Kontur. Um klassische Regelbeispiele stets verbotener Praktiken handelt es sich dabei allerdings nicht. Stattdessen ermächtigt die Norm die Europäische Kommission, für die jeweiligen Konstellationen Leitlinien aufzustellen. Das erlaubt es ihr zwar einerseits, künftig flexibel auf manipulative Gestaltungen zu reagieren. Die Konstruktion schwächt aber andererseits die Rechtssicherheit, da der DSA die Zulässigkeitsgrenzen der Praktiken nicht selbst abschließend klar absteckt.[32]

Art. 25 Abs. 2 DSA formuliert ein zweites Aber: Die Verbotsregeln gelten nur, sofern eine Praxis nicht unter die Richtlinie über unlautere Geschäftspraktiken (UGP-RL)[33] oder die Datenschutz-Grundverordnung (DSGVO)[34] fällt.

Im ersten Zugriff klingt das nach einer starken Einschränkung. Denn die UGP-RL erfasst grundsätzlich eine große Bandbreite an Geschäftspraktiken (Art. 5 Abs. 1, Art. 2 lit. d UGP-RL; vgl. auch für die Umsetzung im deutschen Recht: § 3 Abs. 1, § 2 Abs. 1 Nr. 2 UWG).[35] Genügte es, dass eine konkrete Darstellungsform zugleich als geschäftliche Handlung zu qua-

26 Vgl. Martini/Drews/Seeliger/Weinzierl ZfDR 2021, 47 (53 ff.); Weinzierl NVwZ-Extra 15/2020, 1 (7 ff.).
27 Vgl. Martini/Kramme/Seeliger VuR 2022, 123 (123 f.).
28 Martini/Kramme/Seeliger VuR 2022, 123 (125).
29 Europäische Kommission, Vorschlag für ein Gesetz über künstliche Intelligenz, 21.4.2021, COM (2021) 206 final.
30 Verordnung (EU) 2022/2065 des Europäischen Parlaments und des Rates vom 19.10.2022 über einen Binnenmarkt für digitale Dienste und zur Änderung der Richtlinie 2000/31/EG (Gesetz über digitale Dienste), Abl. L 277 S. 1–102.
31 Verordnung (EU) 2022/1925 des Europäischen Parlaments und des Rates vom 14.9.2022 über bestreitbare und faire Märkte im digitalen Sektor und zur Änderung der Richtlinien (EU) 2019/1937 und (EU) 2020/1828 (Gesetz über digitale Märkte), Abl. L 265 S. 1–66.
32 Anders noch Art. 13a des DSA-E des Parlaments (P9 TA(2022)0014). Er sah neben der Generalnorm eine klassische Katalog-Struktur vor, konnte sich aber im Trilog-Verfahren nicht durchsetzen; vgl. dazu auch Martini/Kramme/Seeliger VuR 2022, 123 (130).
33 Richtlinie 2005/29/EG, insbesondere konkretisiert im UWG.
34 Verordnung (EU) 2016/679, ABl. L 119 S. 1–88.

lifizieren ist, damit die UGP-RL greift, wäre Art. 25 Abs. 1, 3 DSA weitgehend seiner Wirkung beraubt; die neue Vorschrift liefe insbesondere der Mission des DSA zuwider, Onlinedienste „umfassend" zu regulieren.[36] Auch deshalb genügt nicht allein, dass eine „geschäftliche Handlung" vorliegt, um die Ausnahmevorschrift zu aktivieren.

Der normative Verweis auf den Anwendungsvorrang der DSGVO in Art. 25 Abs. 2 DSA verkleinert den Anwendungsbereich der Schutznorm ebenfalls nicht so stark, wie es auf den ersten Blick scheint. Denn so sehr Dark Patterns bei datenschutzrelevanten Einwilligungen auch verbreitet sind, so wenig unterliegen Cookie-Banner als wohl prominentestes Beispiel den Regelungen der DSGVO. Vielmehr gibt insoweit die ePrivacy-RL (bzw. ihre deutsche Umsetzung, das TTDSG) grundsätzlich den rechtlichen Maßstab vor (Art. 95 DSGVO).[37] Art. 25 DSA findet mithin auf Cookie-Banner von Online-Plattformen Anwendung. Für sie stellt Art. 25 Abs. 1, Abs. 3 lit. a DSA (nach dem Vorbild des Art. 7 Abs. 3 Satz 4 DSGVO) klar, dass es ebenso leicht sein muss, alle Cookie-Setzungen abzulehnen wie sie anzunehmen, und schafft in dieser zentralen Frage Rechtssicherheit.[38]

Ergänzend trägt Art. 31 DSA („Compliance by Design") Plattformbetreibern auf, im Verhältnis zu ihren Geschäftspartnern künftig einige allgemeine Vorgaben für Dark Patterns zu beachten. Die Norm (die konzeptuell und hinsichtlich ihres Namens eng an Art. 25 Abs. 1 DSGVO [„Data Protection by Design"] angelehnt ist) verpflichtet Plattformbetreiber dazu, ihr Web-Design so zu gestalten, dass Händler Vertrags- und Informationspflichten einhalten können. Im Kern erkennt Art. 31 DSA somit die organisatorische Verantwortung von Plattformbetreibern in diesem Dreiecksverhältnis an, indem er ihnen verbietet, Händler durch vorgegebene Gestaltungsmöglichkeiten und nicht vorhandene Alternativen dazu zu nötigen, Dark Patterns zu verwenden.

Auch der *Entwurf für eine KI-Verordnung* hält Regelungen vor, die auf den ersten Blick geeignet scheinen, Dark Patterns normativ einzuhegen. Art. 5 KI-VO-E verbietet insbesondere KI-Systeme, die „Techniken der unterschwelligen Beeinflussung außerhalb des Bewusstseins einer Person" einsetzen, „um das Verhalten einer Person […] zu beeinflussen" (Art. 5 Abs. 1 lit. a KI-VO-E). Gleiches gilt für Techniken, die „eine Schwäche oder Schutzbedürftigkeit einer bestimmten Gruppe von Personen" ausnutzen (Art. 5 Abs. 1 lit. b KI-VO-E). Der Tatbestand erfasst allerdings jeweils nur eine solche Form der Beeinflussung, die „einen physischen oder psychischen Schaden" zufügt oder zufügen kann. Durch Dark Patterns ausgelöste Schäden fallen typischerweise nicht hierunter. Bei ihnen handelt es sich regelmäßig um Vermögensschäden. Die KI-VO erfasst das Phänomen in der Entwurfsfassung der Kommission mithin nur in Ausnahmefällen (insbesondere in solchen, in denen Dark Patterns die menschliche Gesundheit verletzen).

Normsystematisch überraschend hält auch der *Digital Markets Act (DMA)* Ansätze für die Regulierung von Dark Patterns vor. Er verfolgt zwar primär marktregulatorische und weniger verbraucherschützende Ziele,[39] nimmt aber auch Umgehungsstrategien in sein regulatorisches Fadenkreuz, die manipulative Oberflächengestaltung einsetzen: Einzelne Dark Patterns finden ihre Schranken bereits in den spezifischen Pflichten des Art. 5–7 DMA – etwa das Verbot, wiederholt durch sog. „Nagging"[40] zur Einwilligung aufzufordern (Art. 5 Abs. 2 UAbs. 2 DMA). Darüber hinaus untersagt Art. 13 Abs. 4 DMA „Verhaltenslenkungsmethoden" oder Schnittstellengestaltung, mit denen Gatekeeper ihre Pflichten aus den Art. 5 bis 7 DMA umgehen könnten. Art. 13 Abs. 6 DMA verlangt zudem, dass Nutzer autonom und mithilfe neutral dargestellter Auswahloptionen entscheiden können, ob sie Dienste von Gatekeepern nutzen wollen. Der DMA formuliert also nicht nur ein materielles Pflichtenprogramm für Gatekeeper, sondern erkennt auch explizit an, dass manipulative Entscheidungsarchitekturen – wie Dark Patterns – seine Regelungen unterlaufen können. Um dies zu vermeiden, verbietet er manipulative Designmuster.

Dark Patterns sind mithin in Summe an vielen Stellen bereits Kernbestandteil neuer Regulierungen und werden in den nächsten Jahren vermehrt die Gerichte beschäftigen. Um insoweit frühzeitig Rechtssicherheit herzustellen, sind klare gesetzliche Leitplanken und Bewertungsmaßstäbe erstrebenswert. Diese tun aber gegenwärtig zum Teil auch in dem neuen unionalen Rechtsrahmen noch not.

IV. Technische Aspekte

Jenseits harter juristischer Vorgaben bergen auch technische Assistenzsysteme das Potenzial, Dark Patterns wirksam zu begrenzen. Schließlich bündeln deren Entscheidungsarchitekturen in Webseiten oder Apps integrierte Daten. Moderne Methoden des Maschinellen Lernens oder der Künstlichen Intelligenz könnten diese Daten analysieren und so verbraucherschädigende Muster detektieren. Nutzern eröffnet dies einen Weg, sich unkompliziert und effektiv gegen Dark Patterns zu wehren. Eine technische Lösung ist auch insofern attraktiv, als diese bereits bei der Entwicklung von Benutzeroberflächen oder Webseiten ansetzen und UX-Designs überprüfen könnte, bevor Verwender sie Nutzern zugänglich machen.

1. Browser-Erweiterungen für Dark Patterns

Viele gängige Web-Browser bieten bereits Erweiterungen (sog. Plugins) an, die Browser um nützliche Funktionen, Einstellungen und Designs ergänzen. Am bekanntesten sind Adblo-

35 Vgl. Martini/Drews/Seeliger/Weinzierl ZfDR 2021, 47 (63 f.); Martini/Kramme/Seeliger VuR 2022, 123 (125).

36 Siehe Digital Services Package: Commission welcomes the adoption by the European Parliament of the EU's. new rulebook for digital services, Pressemitteilung v. 5.7.2022.

37 Für die Regulierung von Cookies ist die DSGVO nur mittelbar aufgrund Verweises relevant (Art. 5 Abs. 3 Satz 1 ePrivacy-RL iVm Art. 94 Abs. 2 DSGVO; § 25 Abs. 1 Satz 2 TTDSG).

38 Vgl. zur bisherigen Diskussion etwa Böhm/Halim MMR 2020, 651 (655); Rauer/Ettig ZD 2021, 18 (22); Sesing MMR 2021, 544 (546).

39 Der DMA adressiert primär Betreiber (zentraler) Plattformen (sog. „Torwächter" / "Gatekeeper", Art. 3 Abs. 1 DMA). Diese bieten eine intermediäre Infrastruktur zwischen Nutzern und dritten Diensten. Dadurch haben sie – etwa als digitale Marktplätze oder Buchungswebseiten – eine besondere Machtstellung inne. In diesem Spannungsfeld soll der DMA einen fairen Wettbewerb sicherstellen.

40 Martini/Drews/Seeliger/Weinzierl ZfDR 2021, 47 (52).

cker, die Werbeanzeigen blockieren. Hier überprüft der Browser, ob der Domainname einer Anzeige (als Teil einer Webseite) auf einer Blacklist steht und zeigt die Werbung in diesem Fall nicht im Browser an.

Insbesondere für Cookie-Banner haben sich in den letzten Jahren einige sehr nützliche Browser-Erweiterungen entwickelt, die zwar nicht direkt Dark Patterns erkennen, aber Cookie-Banner einfach entfernen oder sogar automatisch für Nutzer ausfüllen.[41] Consent-O-Matic[42] ist beispielsweise eine solche, die Verbraucher bemächtigende Anwendung. Sie erkennt Cookie-Banner – basierend auf sog. Consent Management Providern (CMP)[43] – und füllt Einwilligungen nach den Wünschen des Nutzers aus.

Diese Methode, Cookie-Banner zu erkennen und zu handhaben, ist recht gut skalierbar. Denn die Zahl der häufig auf Webseiten verwendeten CMP ist überschaubar. Damit lassen sich aus den Templates entsprechender Einwilligungsformulare der Webseiten zB Regeln für eine automatische Bearbeitung effektiv ableiten und implementieren.

2. Modelle für Dark Patterns und Reaktionen

Ganz so einfach wie für Cookie-Banner ist die Handhabung allgemeiner Dark Patterns nicht. Denn bei ihnen handelt es sich typischerweise um schwer greifbare Teilelemente komplex aufgebauter Webseiten. Ein Dark Pattern lässt sich auf einer Webseite in einer Vielzahl unterschiedlicher Formen darstellen und platzieren. Das UX-Design eröffnet mit heutigen Technologien eine schier grenzenlose Bandbreite an Möglichkeiten, insbesondere wenn man Techniken für dynamische Webinhalte berücksichtigt, die auf Skriptsprachen, wie zB Javascript, basieren. So ist es beispielsweise im Falle eines Patterns des Typs „Sneak into Basket" (Warenkorb-Trick, s. Abbildung 4) nicht damit getan, einfach einige Regeln anzugeben, die eine Browser-Erweiterung nutzt, um zu prüfen, ob eine geladene oder zu ladende Webseite dieses Pattern enthält. Entsprechende explizit aufgeführte Regeln müssten vielmehr alle denkbaren Darstellungsformen kodieren und wären kaum mehr technisch handhabbar.

Abbildung 4: Ein Sneak into Basket"-Pattern, das der Bestellung standardmäßig eine Geschenkkarte hinzufügt.

Es ist daher ein Modell erforderlich, das jedem Element einer Webseite eine Wahrscheinlichkeit zuordnet, die angibt, inwieweit das Element zu einer bestimmten Klasse von Dark Patterns gehört. Aus technischer Sicht handelt es sich somit um ein Daten-Klassifikationsproblem.[44] Ein probabilistischer Ansatz ermöglicht feine Abstufungen für individuelle Typen von Dark Patterns. Bei einem solchen Modell können Nutzer (als Funktion eines entsprechenden Plugins) auch angeben, ab welchem Schwellenwert sie ein Element als Dark Pattern betrachten. Die einzelnen Elemente lediglich rein binär zu klassifizieren (Dark Pattern? – Ja/Nein), ist in den meisten Fällen unzureichend und auch aus rechtlicher Sicht bedenklich. Denn Dark Patterns operieren, beispielsweise im Kontext von Countern, in einem großen Graubereich, in dem sich nicht jedes Element eindeutig einstufen lässt (und auch oft von Nutzern unterschiedlich subjektiv wahrgenommen wird).

Ist ein Element einer Webseite mit hoher Wahrscheinlichkeit als Dark Pattern zu klassifizieren, ist es in den meisten Fällen wenig sinnstiftend, dieses einfach nicht im Browser anzeigen zu lassen. Denn dadurch kann die Website ua einen wichtigen Teil ihrer Funktionalität einbüßen, so dass der Nutzer diese in der Folge nicht mehr sachadäquat verwenden kann. Zudem wäre die durchaus heikle Frage zu beantworten, ob es rechtlich zulässig ist, Inhalte von Webseiten auf diese Weise (automatisch) zu modifizieren.[45]

Eine probate Art und Weise, mit erkannten Dark Patterns umzugehen, besteht darin, diese Elemente auf der Webseite hervorzuheben, zB durch eine farbliche Randmarkierung, die durch Abstufungen des Farbtons auch noch die Wahrscheinlichkeit ausweist, dass ein Element zu einem Dark-Pattern-Typ gehört. Diese Methode modifiziert zwar die Webseite, verändert aber keine Inhalte, sondern lediglich die Darstellungsform (minimal). Obgleich technisch relativ aufwändig, präsentiert sich dies aktuell noch als die geeignetste Form, um (potenzielle) Dark Patterns auf Webseiten kenntlich zu machen. Sie lässt sich überdies in der Weise erweitern, dass ein entsprechendes Browser-Plugin Nutzern die Möglichkeit eröffnet, die automatisch durchgeführte Klassifikation eines

41 Von Bleichert, Cookies automatisch ablehnen: So werden Sie nervige Cookie-Banner los, 27.4.2022, https://www.experte.de/it-sicherheit/cookies-ablehnen (letzter Zugriff am 1.8.2022).

42 Consent-O-Matic, https://consentomatic.au.dk/ (letzter Zugriff am 1.8.2022).

43 CMP sind Drittanbieter von Consent-Management-Werkzeugen, die Betreiber von Webseiten nutzen können, um nicht selbst teils komplexe Masken erstellen zu müssen, mit denen sie Einwilligungen einholen. Dazu Consent Management Plattformen: Welche Angebote gibt es und was können sie?, 18.12.2020, https://www.windrich-soergel.de/blog/consent-management-plattformen-welche-anbieter-gibt-es-und-was-koennen-sie/ (letzter Zugriff am 1.8.2022).

44

45 Der Parallelfall „Werbeblocker" hat in der Vergangenheit bereits einige Gerichte beschäftigt. Sie greifen das digitale Geschäftsmodell an, über die Online-Präsenz Verbraucher zu tracken und personalisierte Werbung auszuspielen. Höchstgerichtlich zuletzt BGH Urt. v. 8.10.2019 – KZR 73/17, MMR 2020, 24 – „Werbeblocker III".

Elements zu bewerten und so die zugrundeliegenden Klassifikationsalgorithmen kontinuierlich zu verbessern.

3. Überwachtes Lernen

Das Klassifikationsproblem, vor dem eine Dark Pattern-App besteht, folgt einem einfachen Aufgabenmuster: Gegeben ist eine Menge von Klassen (Label), von denen eine einem Dark Pattern entspricht. Ziel ist es, ein Modell und dessen algorithmische Umsetzung, den Klassifikator, zu bestimmen, der wiederum ein Element einer Webseite einer Klasse (mit einer Wahrscheinlichkeit) zuordnet. Das Modell bzw. der Klassifikator muss somit typische Instanzen einer jeden Klasse kennen und Merkmale solcher Instanzen geeignet algorithmisch kodieren.

Bei den Verfahren der Klassifikation handelt es sich um überwachte Lernverfahren: Für eine Menge von Instanzen (wobei jede Instanz das Label einer Klasse hat) lernt das System ein Modell, das die typischen Eigenschaften der Instanzen einer Klasse kodiert. Diese vorgegebene Menge an Instanzen mit entsprechenden Klassenlabels bezeichnet man auch als Trainingsdaten. Wie bei allen Klassifikationsverfahren spielen Menge und Qualität der Trainingsdaten für die Validität des Ergebnisses eine sehr wichtige Rolle: Je mehr Trainingsdaten vorhanden sind und je besser die Abdeckung aller Klassen mit Beispiel-Instanzen ist, desto besser kann das Klassifikationsverfahren die Eigenschaften einer jeden Klasse lernen.

Die Verfügbarkeit valider, umfangreicher Trainingsdaten stellt aber auch jeden Ansatz, Dark Patterns-Elemente von Webseiten zu klassifizieren, vor große Herausforderungen. Schon alleine der Prozess, solche Webseiten, die Dark Patterns integrieren, (teils manuell) zu identifizieren, um diese als Trainingsdaten für einen Lernalgorithmus zu verwenden, ist sehr aufwändig.[46] Hierfür ist es erforderlich, das Browsing-Verhalten von Nutzern unter erheblichem technischem Aufwand zu simulieren bzw. zu automatisieren. So gilt es beispielsweise, den Kauf eines Produktes über verschiedene Seiten als Klick-Folge nachzubilden, um dann im Warenkorb abzugleichen, ob hier ein „Sneak into Basket"-Pattern vorliegt.

Viele Dark Patterns zeigen sich erst im Kontext von Nutzer-Interaktionen, wenn zB Nutzer ein bestimmtes Produkt auswählen und dann Elemente auftauchen, die eine Knappheit (Scarcity) oder Kunden-Empfehlungen (Social Proof) präsentieren. Auch eine derartige Auswahl von Produkten muss entweder technisch simuliert oder durch Personen manuell durchgeführt werden – und das für die verschiedensten Formen von Webseiten sowie Darstellungsformen. Hat die Anwendung entsprechende Elemente auf Webseiten detektiert und mit einem Label versehen (was es erforderlich macht, das Element bzw. die zugrundeliegenden Codes aus der Webseite zu extrahieren), sammelt sie diese und führt sie einem Klassifikationsalgorithmus zu. Um die Qualität des Klassifikators anschließend zu evaluieren, braucht es darüber hinaus Testdaten, deren Label zwar bekannt ist, aber die dem Klassifikator als bisher nicht klassifizierter Dateninput dienen. Mit ihrer Hilfe lässt sich dann unkompliziert überprüfen, ob der Klassifikator die richtige Klassen- bzw. Pattern-Zuordnung vorgenommen hat. Klassifikationstechniken entpuppen sich mithin (auch als Bestandteil eines Plugins) als Goldstandard, um Dark Patterns zu erkennen; die notwendigen Trainings- und Testdaten lassen sich aber nur sehr aufwändig erstellen.

Selbst wenn eine vollumfängliche technische Lösung, die Dark Patterns automatisch erkennt, in absehbarer Zeit nicht zur Verfügung stehen wird, finden sich Wege, die unterstützend wirken können. Ein erfolgversprechender Ansatz basiert auf der „Wisdom of the Crowd", wie er zB auch zum Einsatz kommt, um Spam-E-Mails zu enttarnen: Nutzer geben einem System Feedback, damit dieses sein Modell verbessern oder anpassen kann. Markiert beispielsweise der Nutzer eine E-Mail als Spam, so lernt das zugrundeliegende System (binäre Klassifikation von E-Mails: Spam? – Ja/Nein) Eigenschaften von Spam-E-Mails. Eine solche Methodik eignet sich auch für Dark Patterns. Entdeckt eine autorisierte Person ein Dark Pattern auf einer Webseite, erlaubt ein Plugin, ein solches Element auf der Webseite zu annotieren. Das System extrahiert daraufhin das Webseitenelement und führt dies dem Klassifikator zu, der im Anschluss das Modell entsprechend anpasst. Je häufiger Nutzer ein Element einer Webseite als Dark Pattern markieren, desto sicherer kann der Klassifikator ähnliche Elemente auf anderen Webseiten klassifizieren. Allerdings sollte auch hier die Anwendung auf eine Basismenge an bereits gelabelten Trainingsdaten zurückgreifen können, um auf der Grundlage weiterer von Nutzern angegebener Daten bzw. Elemente schnell zu hochwertigen Klassifikationsergebnissen zu kommen.

Um Missbrauch und Meinungsbeeinflussung zu begrenzen, könnten die kollektiven Bewertungssysteme die Reputation der Bewerter öffentlich machen oder sie zumindest systemintern beobachten oder incentivieren. Weiterhin kann es motivierend wirken, den Vertrauensgrad der bewerteten Dark Patterns anzuzeigen, damit selten bewertete Dark Patterns ebenfalls Aufmerksamkeit erhalten. Obgleich diese Methode einige technische Herausforderungen birgt, liefert sie in Summe eine adäquate Strategie, um auch neue Dark Patterns zu erlernen und somit der Dynamik von Webinhalten gerecht zu werden.

VI. Zusammenfassung und Ausblick

Dark Patterns sind Ausdruck eines Machtungleichgewichts zwischen Anbietern und Nutzern einer Webseite. Mit ihrer Hilfe gestalten große Konzerne und Plattformen die digitale Umwelt einseitig im Sinne ihrer wirtschaftlichen Interessen aus. Auf der Grundlage ihrer sich stetig weiter füllenden Datensilos können die Anbieter Hypothesen über Schwächen menschlichen Verhaltens aufstellen und unmittelbar validieren. Für den einzelnen Nutzer materialisiert sich dies in einer individuellen digitalen Oberfläche. Alles, was darunter oder auf kollektiver Ebene passiert, bleibt ihm verborgen. Diese Schlagkraft digitaler Designmuster stellt auch die Wissenschaft sowie die Regulierungsbehörden und Verbraucherschutzverbände vor Herausforderungen. Ein geschärftes Verständnis der Hintergründe, Reichweite und Implikationen

46 Mathur/Acar/Friedman/Lucherini/Mayer/Chetty/Narayanan Proceedings of the ACM on Human-Computer Interaction 2019, Article No. 81, S. 1.

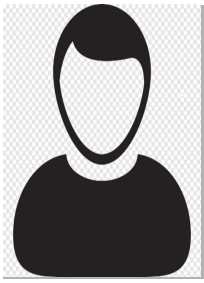
digitaler Beeinflussung ist essenziell, um gemeinsam die künftigen Spielregeln im digitalen Raum auszuhandeln.

So sehr digitale Innovationen der Menschheit viel Nutzen gestiftet haben, so sehr ist es unerlässlich, Designer sowie Informatiker für die Macht zu sensibilisieren, die sie in den Händen halten. Um eine neue digitale Normalität zu schaffen, ist auch eine klare, Rechtssicherheit schaffende Regulierung von Dark Patterns geboten. Den bisherigen Ansätzen auf nationaler sowie unionaler Ebene gelingt dies nur eingeschränkt. Für Dark Patterns bedarf es weiterer passgenauer gesetzlicher Regelungen. Flankierend gilt es, technische Lösungen auszubauen, die ihnen begegnen, und das zivilgesellschaftliche Engagement gegen beeinflusste Konsumentscheidungen zu stärken. Nur wenn alle Akteure zusammenwirken, gelingt es, die „dunkle Seite des Designs" – für alle hinreichend sichtbar – aus der Dunkelheit ans Licht zu bringen.

Die Regulierung von Inkassodienstleistungen nach dem sog. Legal Tech-Gesetz

Dr. Charlotte Flory

Das Gesetz zur Förderung verbrauchergerechter Angebote im Rechtsdienstleistungsmarkt aus dem Jahr 2021 hat nicht nur mehr Rechtssicherheit für Legal Tech-Inkassounternehmen gebracht, sondern auch die damit in Zusammenhang stehende Regulierung von Inkassodienstleistern insgesamt verschärft. Hierdurch sollte einerseits der Verbraucherschutz verbessert werden[1] und andererseits die ungleiche Regulierung von inkassodienstleistenden Rechtsanwälten und reinen Inkassodienstleistern im Bereich des Legal Tech-Inkassos abgebaut werden.[2] In der wissenschaftlichen Debatte standen bei der Diskussion um die unterschiedliche Regulierung von der Rechtsanwaltschaft und registrierten Inkassodienstleistern vor allem die Berufspflichten für die Rechtsanwaltschaft im Fokus. In diesem Beitrag soll die Regulierung der Inkassodienstleister im Vordergrund stehen, indem die neuen Regulierungsansätze aus dem Gesetz zur Förderung verbrauchergerechter Angebote im Rechtsdienstleistungsmarkt vorgestellt und in die wissenschaftlichen Streitfragen entsprechend eingeordnet werden.



Die Autorin ist Syndikusrechtsanwältin und war zuvor mehrere Jahre promotionsbegleitend im Europäischen Zentrum für Freie Berufe der Universität zu Köln beschäftigt.

I. Hintergrund der neuen Regelungen für Inkassodienstleister

Die gewerbliche Inkassodienstleistung war berufsrechtlich bislang bewusst nicht stark reguliert.[3] Inkassodienstleister hatten auf dem Markt die wesentliche Funktion der Forderungsdurchsetzung inne,[4] die sie insbesondere durch das klassische Masseninkasso umsetzten, also die massenhafte Durchsetzung fremder Forderungen. Zwar war seit einer Entscheidung des BVerfG aus dem Jahr 2002 klar, dass die Inkassotätigkeit auch die rechtliche Beratung über die Forderungen umfasste.[5] Allerdings ist erst durch das Legal Tech-Inkasso das Element der Rechtsberatung bei der Inkassodienstleistung umfassend in den Vordergrund gerückt. Deshalb ist die Rechtsdienstleistung im Bereich der Forderungsdurchsetzung durch Legal Tech-Inkassounternehmen in vielen Aspekten identisch mit der Rechtsdienstleistung, die Rechtsanwälte herkömmlich erbrachten,[6] insbesondere in den Bereichen des Verkehrsrechts oder Mietrechts[7]. Rechtsanwälte waren und sind im Gegensatz zu den Inkassodienstleistern allerdings an die strenge Regulierung des anwaltlichen Berufsrechts gebunden.[8] Deshalb durften sie beispielsweise wegen § 49b Abs. 2 S. 1 BRAO iVm § 4a Abs. 1 S. 1 RVG aF kein generelles Erfolgshonorar vereinbaren, wohingegen diese Wette auf den eigenen Erfolg den Geschäftserfolg der Legal Tech-Inkassounternehmen maßgeblich steigerte.[9] Dass Rechtsanwälte gleichzeitig sowohl als Organe der Rechtspflege berufen sind, als auch eine langjährige theoretische und praktische Ausbildung vorweisen können, wurde zurecht von vielen Seiten als inkohärent und reformbedürftig kritisiert.[10] Das Gesetz zur Förderung verbrauchergerechter Angebote im Rechtsdienstleistungsmarkt wollte Abhilfe leisten und sowohl Wettbewerbsnachteile für Rechtsanwälte im Bereich der Inkassodienstleistungen abschaffen[11] als auch den Verbraucherschutz durch strenge Regulierung der Inkasso-

1 BT-Drs. 19/27673, S. 13.
2 BT-Drs. 19/27673, S. 13.
3 BT-Drs. 16/3655, S. 31f.
4 Flory, Grenzen zulässiger Inkassodienstleistungen, S. 10.
5 BVerfG 20.2.2002 – 1 BvR 423/99, 1 BvR 821/00 und 1 BvR 1412/01, NJW 2002, 1190 (1191).
6 Deckenbrock/Henssler, in: Deckenbrock/Henssler Rechtsdienstleistungsgesetz, 5. Auflage 2021, § 2 Rn. 95b.
7 Zu den Rechtsgebieten, in denen Legal Tech-Unternehmen derzeit etabliert sind, Kilian AnwBl Online 2021, 608 (609).
8 Die in Zusammenhang mit Inkassodienstleistungen für Rechtsanwälte bestehenden Pflichten aufzählend Fries NJW 2021, 2537 (2539).
9 Zu den Wettbewerbsvorteilen BT-Drs. 19/27673, S. 13; Henssler NJW 2019, 545 (545); Kilian AnwBl Online 2021, 608 (609).
10 Fries NJW 2021, 2537 (2538); Hellwig AnwBl Online 2020, 260 (261); Kilian NJW 2019, 1401 (1405).
11 BT-Drs. 19/27673, S. 13.