Dark Patterns

Phänomenologie und Antworten der Rechtsordnung

Prof. Dr. Mario Martini/Christian Drews/Paul Seeliger/
*Quirin Weinzierl, LL.M. (Yale)**

In der Welt digitaler Benutzeroberflächen begegnen Nutzer immer häufiger sog. „Dark Patterns", die Entscheidungen ihrer Adressaten subtil in eine bestimmte Richtung lenken. Wer Webseiten aufruft, stellt etwa fest, dass es deutlich leichter ist, Berechtigungen für Cookies zu erteilen, als diese zu verweigern. Der Beitrag leuchtet die bestehenden rechtlichen Grenzen, aber auch Lücken für Dark Patterns im Datenschutz-, Vertrags- und Lauterkeitsrecht aus.

Inhaltsübersicht

ZfDR 2021, 47–74

„Das Angebot ist nur noch 60 Sekunden zum angegebenen Preis reserviert!" Bis vor Kurzem sah eine derartige Meldung, wer eine der größten weltweiten Hotelvermittlungs-Websites nutzte. Mutige Kunden, die die Probe aufs Exempel machten und die Warnung ignorierten, merkten jedoch, dass der Zeitablauf keinerlei Konsequenzen nach sich zog.[1] Der geforderte Preis blieb identisch und der Urlauber konnte die Buchung zu denselben Konditionen fortführen. Der Anbieter setzte also darauf, Kunden mit Hilfe vorgetäuschten zeitlichen Drucks dazu zu drängen, einen Vertrag abzuschließen.[2]

Der Fall steht paradigmatisch für viele andere Praktiken, mit denen Anbieter das Verhalten ihrer Nutzer in digitalen Umgebungen zu steuern versuchen. Designmuster wie der Reservierungs-Countdown finden (zumindest international) unter der Bezeichnung „Dark Patterns" vermehrt öffentliche Aufmerksamkeit. Den Begriff prägte der Interfacedesign-Spezialist *Harry Brignull* im Jahr 2010.[3] Die Forschung, vornehmlich aus dem Bereich des Interfacedesigns, richtet ihr analytisches Mikroskop seither immer stärker darauf, lenkende Designmuster anhand von Beispielen zu beschreiben und zu kategorisieren, die Verbreitung und Wirksamkeit der Praktiken zu belegen sowie Techniken zu entwickeln, um Dark Patterns automatisiert zu erkennen.[4]

Bei manchen Behörden und einigen Politikern wirkten diese Untersuchungen als Weckruf. So hat die US-amerikanische *Federal Trade Commission* (FTC) im September 2020 gegen die digitale Lernplattform „Age of Learning" wettbewerbsrechtliche Maßnahmen wegen Dark Patterns ergriffen.[5] Nahezu zeitgleich legte die Datenschutzbehörde des Vereinigten Königreichs (ICO) einen neuen Standard für altersangemessenes Design vor, der spezifische verhaltensbeeinflussende Techniken allgemein verbietet.[6] Auch legislative Maßnahmen zeichnen sich ab: Der sog. DETOUR Act[7], den Senatoren des US-Kongresses parteiübergreifend in den Senat eingebracht haben, ist mit dem Ziel angetreten, Online-Verhaltensbeeinflussungen, insbesondere Dark Patterns, zu verbieten. Kalifornien hat in den *California Privacy Rights Act of 2020* (CPRA) sogar explizit eine Bestimmung aufgenommen, die festschreibt, dass Zustimmungen

---

* *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. *Christian Drews* und *Paul Seeliger* sind Forschungsreferenten, *Quirin Weinzierl* ist Koordinator in dem „Dark-Pattern-Detection-Project" (Dapde), welches das BMJV fördert. Die Autoren danken *Anton Kamke, Carolin Heinzel, Jule Martenson* und *Ulrike Urbanek* für ihre sehr gute Unterstützung. Soweit nicht anders vermerkt, sind Internetquellen auf dem Stand vom 10.1.2021.

[1] Vgl. auch *Bundeskartellamt*, Sektoruntersuchung Vergleichsportale, 2019, S. 107 f.

[2] Auf Drängen der Europäischen Kommission und der nationalen Verbraucherschutzbehörden hin erklärte der Anbieter schließlich, bis Mitte 2020 auf diese Praxis zu verzichten; vgl. *Europäische Kommission,* Nach Intervention der EU verpflichtet sich Booking.com, die Darstellung von Angeboten und Preisen mit dem EU-Recht in Einklang zu bringen, Pressemitteilung v. 20.12.2019; MMR-Aktuell 2020, 424225.

[3] *Brignull/Darlo*, Dark Patterns – Types of Dark Pattern, abrufbar unter: darkpatterns.org/types-of-dark-pattern, auch mit einer Beispielsammlung.

[4] Etwa *Mathur/Acar et al.,* PACM HCI 2019, Article 81, 1.

[5] *Federal Trade Commission,* Regarding Dark Patterns in the Matter of Age of Learning, Inc., Pressemitteilung v. 2.9.2020.

[6] *UK Information Commissioner's Office*, Age Appropriate Design: A Code of Practice for Online Services, 2020, S. 72 ff.

[7] Deceptive Experiences To Online Users Reduction (DETOUR) Act, S. 1084, 116th Cong. (2019). Mittlerweile ist der Gesetzentwurf hinfällig.

zu Datenverarbeitungen, die der Anbieter mit Hilfe von Dark Patterns erlangt hat, unwirksam sind.[8]

In Deutschland hingegen haben Dark Patterns sowohl in der Rechtswissenschaft als auch in der Aufsichtspraxis bisher nur sehr verhaltene Aufmerksamkeit erfahren.[9] Auch hier steht die Rechtsordnung aber vor der Frage, ob und inwieweit Regulierungsbedarf besteht.

I. Das Phänomen „Dark Patterns"

1. Gängiges Begriffsverständnis

Der Terminus „Dark Pattern" ist ein Sammelbegriff, unter dessen Dach sich viele, teils unterschiedliche Phänomene tummeln. Eine einheitliche Definition hat sich bisher (noch) nicht herausgebildet. Ein gemeinsamer Kern schält sich gleichwohl heraus: Bei Dark Patterns handelt es sich um digitale Designmuster, die Nutzer zu Handlungen verleiten, welche ihren „eigentlichen" Interessen zuwiderlaufen oder die sie andernfalls nicht vorgenommen hätten.[10] Neben Countdowns, die Angebote (mitunter scheinbar) zeitlich befristen, sind auch Verweise auf die (vermeintliche) Knappheit und das (vermeintliche) Verhalten anderer Nutzer typische Erscheinungsformen – ebenso wie graphische Hervorhebungen, welche die Aufmerksamkeit lenken. Weitere Anwendungsbeispiele sind voreingestellte Eingabemöglichkeiten sowie suggestive Fragen und Informationen.

Dark Patterns sind besondere Spielarten von *Design Patterns*. Deren Konzept stammt ursprünglich aus der Architektur.[11] Design Patterns beschreiben Vorlagen für häufig wiederkehrende Gestaltungsaufgaben.[12] Designer bedienen sich ihrer etwa, um Oberflächen und Bedienelemente für Nutzer nachvollziehbar zu gestalten (sog. *User-Interface-[UI-]Design)*. Ganze digitale (Um-)Welten basieren auf ihnen.

Ebenso wie andere Designmuster sind Dark Patterns zwar fest in ihre Umgebung eingewoben. Von herkömmlichen Mustern unterscheiden sie sich jedoch dadurch, dass sie Nutzer zu einem Handeln, Dulden oder Unterlassen verleiten, indem sie Reflexionslücken der präferenzgerechten, rationalen menschlichen Entscheidungsfindung ausnutzen.

2. Wirksamkeit und -mechanismen

Aus Anwenderperspektive gilt als „harte Währung" von Dark Patterns ihre Wirksamkeit. Einen Beeinflussungserfolg im Einzelfall setzen Dark Patterns gleichwohl nicht zwingend voraus – schon deshalb, weil unter der Vielzahl adressierter Nutzer einige für Verhaltensbeeinflussung besonders sensibilisiert sein können. Dark Patterns

---

[8] Sec. 14 lit. h CPRA, zur Änderung von Sec. 1798.140 lit. h Nr. 1 *Cal. Civil Code* (*California Consumer Privacy Act* 2018, CCPA). Zum CPRA allgemein *Lejeune,* ITRB 2021, 13 (13 ff.).

[9] So etwa *Hill* DÖV 2020, 205 (206); *Weinzierl* NVwZ-Extra 15/2020, 1 (1 ff.).

[10] Vgl. die Definitionen bei: *Bogenstahl*, Dark Patterns, 2019, S. 1: „die deren eigentlicher Intention zuwiderlaufen", „Nachteile oder negative Konsequenzen"; *Brignull/Darlo*, Dark Patterns – Types of Dark Pattern, abrufbar unter: darkpatterns.org/types-of-dark-pattern: „things that you didn't mean to"; *Forbrukerrådet*, Deceived by Design, 27.6.2018, S. 7: „not in their interest"; *Gray/Kou et al.,* CHI 2018, Paper 534, 1 (1): „not in the user's best interest"; *Luguri/Strahilevitz*, Shining a Light on Dark Patterns, 2019, abrufbar unter: https://ssrn.com/abstract=3431205, S. 11: „things they would not otherwise do".

[11] *Alexander/Ishikawa et al.*, A pattern language, 1977, S. x.

[12] *Gamma/Helm et al.*, Design Patterns, 2015, S. 27 ff.

sollen ihrem Wesen nach auch nicht spezifische Personen, sondern vielmehr eine hinreichende Anzahl von Menschen beeinflussen. Dementsprechend sind Dark Patterns über-individuell zu bestimmen: Es genügt, dass Gestaltungen eine kritische Mindestanzahl menschlicher Entscheidungen im Sinne ihres Verwenders beeinflussen können.

Der Mechanismus, durch den sie wirken, ist demgegenüber sekundär: Sie können manipulieren, täuschen, nötigen oder Nutzer steuern.[13] Der überwiegende Teil der beobachteten Phänomene macht sich verhaltensökonomische bzw. -psychologische Effekte zunutze.[14] *Scarcity*- und *Countdown*-, *Preselection*- sowie *Trick Question*-Patterns etwa instrumentalisieren *Biases* und *Heuristiken* der Entscheider.[15] Andere Dark Patterns basieren auf Elementen der (empirischen) Designforschung[16] oder disziplinübergreifenden Mischgebilden.[17]

Die Wirkmechanismen von Dark Patterns beschränken sich keineswegs auf die digitale Welt. Sie sind bspw. ebenso in Gestalt des Arrangements von Supermarktregalen im Kassenbereich[18] oder des absichtlich verbreiteten Geruchs frischer Backwaren als Kaufanreiz denkbar.[19] Das digitale Umfeld bietet für solche Beeinflussungsstrukturen jedoch ein optimales Ökosystem – insbesondere um Interfacegestaltungen zu erproben. Denn in der digitalen Welt können entscheidungssteuernde Konstrukte tendenziell mächtiger und nuancierter wirken als ihre nicht-digitalen Pendants:[20] Digitale Umgebungen lassen sich nicht nur fast beliebig gestalten, sondern auch kurzfristig sowie zu niedrigen Kosten anpassen. Gerade reichweitenstarke Online-Anbieter können im laufenden Betrieb kleinste Oberflächen-Veränderungen an ihren Nutzern testen und dadurch die Wirksamkeit ihrer Designelemente erhöhen (sog. *A/B-Testing*).[21] Auf diese Weise ist es ihnen möglich, kontinuierlich den Einfluss von Maßnahmen – etwa auf die Verweildauer, die Anzahl der Einwilligungen und Vertragsabschlüsse von Nutzern oder die generelle Reichweite der Seite – zu überprüfen und ggf. zu steigern.

Derartige Tests validieren nicht nur, *ob* Dark Patterns wirken, sondern auch *bei wem*. Sie erzielen nämlich bei Menschen mit verschiedenen Eigenschaften und Hintergründen unterschiedliche Effekte. Attribute wie etwa der Bildungsstatus oder die politische Einstellung[22] sowie (wohl) auch das Geschlecht[23] korrelieren sowohl mit dem Grad der generellen und situativen Beeinflussbarkeit eines Nutzers als auch der Wirksamkeit

[13] *Jaiswal*, Dark patterns in UX: how designers should be responsible for their actions, UX Collective vom 16.4.2018: „manipulate", „tricking"; *Mathur/Acar et al.,* PACM HCI 2019, Article 81, 1 (2): „coercing", „steering"; *United States Senator for Nebraska Deb Fischer,* Senators introduce bipartisan legislation to ban manipulative 'dark patterns', Pressemitteilung v. 9.4.2019: „manipulate".

[14] *Gray/Kou et al.,* CHI 2018, Paper 534, 1 (1): „use their knowledge of human behavior"; *United States Senator for Nebraska Deb Fischer* (o. Fn. 13): „drawn from extensive behavioral psychology research".

[15] Vgl. *Baek/Bae et al.,* The Social Science Journal 2014, 523 (528 ff.). Zu den Konzepten *Kahneman/Tversky,* Econometrica 1979, 263; *Tversky/Kahneman,* Science 1974, 1124.

[16] Etwa *Chittaro*, in: Meschtscherjakov/Ruyter/Fuchsberger et al. (Hrsg.), Persuasive Technology, 2016, S. 6 ff.; *Mandel/Johnson,* J Consum Res 2002, 235 (237 ff.).

[17] Auffällig ist zudem, dass Dark Patterns regelmäßig das assoziative und unterbewusste System 1-Denken ansprechen; *Luguri/Strahilevitz* (o. Fn. 10), S. 3. Vgl. *Evans,* Trends in Cognitive Sciences 2003, 454 (454 ff.).

[18] Vgl. *Thaler/Sunstein*, Nudge, 2008, S. 1 f.

[19] Vgl. auch *Hacker*, Verhaltensökonomik und Normativität, 2017, S. 662 f.

[20] Vgl. *Luguri/Strahilevitz* (o. Fn. 10), S. 22.

[21] S. *Narayanan/Mathur et al.,* acmquere 2020, 67 (80); *Susser/Roessler et al.,* Georgetown Law Technology Review 2019, 1 (29 ff.); *Yeung,* Information, Communication & Society 2017, 118 (122).

[22] *Luguri/Strahilevitz* (o. Fn. 10), S. 27 f.

[23] Unterschiedliche Farben auf Webseiten wirken bspw. themenspezifisch bei Männern anders als bei Frauen; *Chittaro*, in: Meschtscherjakov/Ruyter/Fuchsberger et al. (o. Fn. 16), S. 8 ff.

spezieller Patterns. Digitale Tracking-Methoden vereinfachen es Verantwortlichen, diese persönlichen Parameter zu erheben. Perspektivisch ist es dadurch möglich, Web-Oberflächen auf jeden Besucher individuell zuzuschneiden, um maximale Wirksamkeit zu erreichen (sog. *Personalized Dark Patterns*[24]).[25] So lassen sich nicht nur Nutzer mit ihren jeweiligen Schwächen gezielt ansprechen; eine Personalisierung macht es zudem ungleich schwieriger, Dark Patterns aufzufinden und zu verfolgen.

3. Kategorisierung

Die Interfacedesignforschung unternimmt Versuche, verschiedene Arten der Muster zu kategorisieren. *Brignull* selbst beschreibt zwölf verschiedene Typen von Dark Patterns, die er teilweise selbsterklärend (*Trick Question*, *Hidden Costs*, *Disguised Ads*) und in anderen Fällen kreativ (*Privacy Zuckering*[26], *Roach Motel*[27]) benennt.[28] Andere strukturieren und verfeinern *Brignulls* Typen-Katalog, indem sie Oberbegriffe (*Nagging*, *Obstruction*, *Sneaking*, *Interface Interference* und *Forced Action*) und weitere Typen einführen.[29] Aus den vorhandenen Ansätzen lässt sich eine an der Wirkungsweise orientierte konsolidierte Klassifizierung destillieren (s. Tabelle auf der Folgeseite).

4. Abgrenzung zum Nudging

Indem Dark Patterns vielfach auf verhaltensökonomische Steuerungseffekte und Biases zurückgreifen, wohnt ihnen eine Wesensverwandtschaft zum *Nudging* und anderen Phänomenen der Verhaltenssteuerung inne. Sie unterscheiden sich von ihnen aber in ihrem Zweck bzw. Erfolg: *Nudging* will Nutzern zu Entscheidungen verhelfen, die ihren vermuteten eigenen mittel- oder langfristigen Präferenzen entsprechen oder zumindest gesamtgesellschaftliche Ziele fördern.[30] Dark Patterns hingegen setzen sich über individuelle Präferenzen hinweg oder ignorieren sie jedenfalls. Sie beeinflussen menschliche Entscheidungen allein zugunsten der Agenda ihres Verwenders.[31] Man kann daher auch von *Dark Nudging*[32] sprechen.

---

[24] *Weinzierl* NVwZ-Extra 15/2020, 1 (3).

[25] *Susser/Roessler et al.,* Internet Policy Review 2019, 1 (31 f.); *Yeung,* Information, Communication & Society 2017, 118 (121 f.). Entsprechende Auswertungen lassen sich allerdings nicht nur zu kommerziellen Zwecken nutzen; *Roßnagel* MMR 2020, 222 (225).

[26] Verleitung zum extensiven, unbedachten Teilen persönlicher Daten (in Anspielung auf *Mark Zuckerberg*).

[27] „Schabenfalle": Nutzerkontos lassen sich mühelos erstellen, sie zu löschen oder sich von dem Dienst abzumelden, erschwert der Anbieter jedoch durch komplizierte Menüführung oder weitere Handlungserfordernisse, wie eine zwingende telefonische Kontaktaufnahme.

[28] *Brignull/Darlo*, Dark Patterns – Types of Dark Pattern, (o. Fn. 3).

[29] Vgl. *Gray/Kou et al.,* CHI 2018, Paper 534, 1 (4 ff.); *Mathur/Acar et al.,* PACM HCI 2019, Article 81, 1. Allen Klassifikationen ist gemein, dass sie nur Näherungswerte abbilden und vielfache alternative Einteilungsformen (zB nach dem Grad der Wirksamkeit oder dem erzielten Nutzerverhalten) denkbar sind. So lässt sich etwa eine *Hidden Subscription* (auch) durch eine Vorauswahl von Häkchen, eine *Trick Question* oder eine Kombination aus beiden erreichen; ob der Mechanismus täuscht, etwas erschleicht oder wegen höherer Transaktionskosten ein zusätzliches Hindernis errichtet, hängt vom Einzelfall ab.

[30] *Thaler/Sunstein* (o. Fn. 18), S. 107 ff.; vgl. auch *Seckelmann/Lamping* DÖV 2016, 189 (193); *Smeddinck* ZRP 2014, 245 (246).

[31] Vgl. *Luguri/Strahilevitz* (o. Fn. 10), S. 3.

[32] Vgl. etwa *Weinzierl* NVwZ-Extra 15/2020, 1 (3).

Kategorie	Druck	Operativer Zwang	Hindernisse	Erschleichen	Irreführen
Wirkungsweise	Ein Designmuster setzt den Nutzer **unter Druck**, eine bestimmte Handlung (nicht) vorzunehmen	**Keine Entscheidungsmöglichkeit** oder (mindestens) eine Entscheidungsalternative ist an **weitere Bedingungen** geknüpft	Bestimmte Entscheidungsmöglichkeiten auszuüben, erfordert **unnötigen/zusätzlichen Aufwand**	Der Nutzer bemerkt die Konsequenzen seiner Handlung aufgrund **heimlicher Änderungen** nicht	Gestaltung der Benutzeroberfläche, die übliche **Erwartungen enttäuscht** bzw. ihnen entgegenläuft
Beispiele[33]	**Nagging** (#): wiederholtes (aggressives) Auffordern, eine bestimmte Handlung vorzunehmen	**Forced Enrollment** (+): Nutzung eines Service nur bei Abschluss eines Abos/Kundenkontos	**Roach Motel** (*, #, +): Anmeldung/Abonnieren wesentlich einfacher als Kündigung	**Sneak into Basket** (*, #, +): Zusätzliches Objekt landet ungewollt im Warenkorb	**Trick Question** (*, #, +): verwirrend formulierte Frage (zB doppelte Verneinung)
	Confirmshaming (*, +): Die Auswahlgestaltung einer Frage löst Schuldgefühle aus	**Forced Continuity** (*, #): automatisches Abonnement; Kündigung erschwert	**Preselection** (#): Auswahlmöglichkeiten sind bereits (abänderbar) getroffen, insbes. durch gesetzte Häkchen	**Hidden Costs** (*, #, +): Zusatzkosten erscheinen erst im letzten Bestellschritt	**Misdirection** (*, +): Design lenkt durch auffällige graphische Elemente vom Inhalt ab
	Countdown (+): Ware/Dienstleistung (angeblich) nur für bestimmte Zeit verfügbar	**Forced Review**: Nutzer können einen Dienst nur dann weiterhin nutzen, wenn sie ad hoc etwa (geänderte) Datenschutzeinstellungen durchsehen und ggf. akzeptieren	**Hidden Information** (#): Für den Nutzer relevante Informationen sind versteckt oder nur schwer verfügbar	**Hidden Subscription** (+): automatisches Abonnieren von Leistungen/Angeboten	**Bait and Switch** (*, #): Klick auf Schaltfläche führt zu anderem Ergebnis als üblicherweise erwartet
	Scarcity (+): Ware/Dienstleistung (angeblich) nur in knapper Zahl verfügbar		**Price Comparison Prevention** (*, #): Preisvergleich erschwert (zB Fremdwährung)		**Disguised Ads** (*, #): als Inhalt oder Steuerungselement getarnte Werbung
	Social Proof (+): direktes Einblenden von (gefälschten) Kundenbewertungen oder dem (vermeintlichen) Verhalten anderer		**Click Fatigue**: Klickwege zu verschiedenen Optionen sind unterschiedlich lang („Klickmüdigkeit")		

5. Kritik an bisherigen Definitionsansätzen und Lösungsvorschlag

Die bisherigen Definitionsansätze zu Dark Patterns bleiben eine klare Antwort auf die Frage schuldig, was das „Dunkle" an ihnen eigentlich ausmacht. Sie lassen insbesondere offen, inwiefern die Wirkung eines bestimmten Designs verwerflicher ist als etwa die (im Grundsatz gesellschaftlich akzeptierte und rechtlich zulässige) werbende Darstellung eines Produkts. Der am häufigsten genutzte Definitionsansatz, der auf die Frustration der „eigentliche[n] Interessen"[34] abstellt, greift insoweit zu kurz. Nicht zuletzt lässt sich nicht immer zuverlässig messen, was im Einzelfall substanziell „gewollt" ist bzw. den „Interessen" der Nutzer entspricht. So können bspw. kurzfristige und langfristige Interessen auseinanderfallen.

Schaut man genauer hin, ist allen Dark Patterns ein Merkmal gemein, das sie von sonstigen Steuerungsmechanismen abgrenzbar macht: Ihre Verwender nutzen die Ge-

[33] Die Bsp. finden sich auch, teilweise unter ähnlichem Namen, bei: (*) *Brignull/Darlo*, Dark Patterns – Types of Dark Pattern (o. Fn. 3); (#) *Gray/Kou et al.,* CHI 2018, Paper 534, 1; (+) *Mathur/Acar et al.,* PACM HCI 2019, Article 81, 1.

[34] So etwa *Bogenstahl* (o. Fn. 10), S. 1. Vgl. auch *Gray/Kou et al.,* CHI 2018, Paper 534, 1 (1); *Susser/Roessler et al.,* Internet Policy Review 2019, 1 (7).

staltungsmacht über Benutzeroberflächen unangemessen zum eigenen Vorteil aus; sie lenken nicht nur menschliches Verhalten, sondern agieren zugleich *missbräuchlich*.[35] Dark Patterns setzen die Interessen ihrer Verwender mithin einseitig gegen die Interessen des Nutzers durch – insbesondere um eine höhere Zahl von Vertragsabschlüssen oder -verlängerungen zu generieren, höhere Interaktionsraten zu erreichen oder mehr Daten zu sammeln, die sich letztlich über Werbung monetisieren lassen. Ein Indiz für Missbräuchlichkeit sind solche Gestaltungen, welche die Bedienbarkeit für Nutzer hinsichtlich einer Entscheidungsoption erheblich schmälern und nicht oder nur untergeordnet durch die Funktionalität des Dienstes angezeigt sind.[36] Gleiches gilt für Gestaltungen, die so ungewöhnlich sind, dass der Verbraucher typischerweise nicht mit ihnen zu rechnen braucht.[37]

Missbräuchlichkeit impliziert nicht automatisch ein vorsätzliches Handeln oder gar eine Schädigungsintention, auch wenn einige Definitionsvorschläge[38] zusätzlich eine derartige subjektive Komponente fordern. Dark Patterns können vielmehr ebenso unbeabsichtigt entstehen – insbesondere, wenn Anwender lediglich die Wirkung einzelner Gestaltungselemente (ggf. vollständig automatisiert) erhöhen. Überdies ist von außen betrachtet vielfach nicht erkennbar, ob Vorsatz vorliegt. Zu welchem Grad Dark Patterns Entscheidungen bewusst oder gewollt beeinträchtigen, ist für eine wirkungsorientierte Qualifikation ohnehin unerheblich.[39]

Dark Patterns sind also in conclusio alle Designmuster, die eine kritische Zahl an Nutzern zu einem bestimmten Verhalten verleiten und dabei die Gestaltungsmacht über Benutzeroberflächen einseitig im Interesse ihrer Verwender ausnutzen.

II. Antworten der Rechtsordnung

Die deutsche wie die unionale Rechtsordnung greifen das Phänomen der Dark Patterns bislang nicht explizit auf. Unterschiedliche rechtliche Sphären schieben missbräuchlichen Beeinflussungen durch Oberflächen jedoch zumindest partiell einen Riegel vor. So versagt etwa das Datenschutzrecht Einwilligungen, die das Ergebnis von Dark Patterns sind, uU die Wirksamkeit; das Zivilrecht kann vertragsrechtliche Willenserklärungen für ungültig erklären. Wer Dark Patterns nutzt, ist zudem womöglich lauterkeitsrechtlich belangbar oder riskiert sogar eine Betrugsstrafbarkeit.

1. Verfassungsrecht

Ebenso wie sonstige absatzfördernde Kommunikation, insbesondere Werbung, sind Dark Patterns Ausdruck grundrechtlich geschützten Verhaltens.[40] Der Staat hat die Pri-

[35] Ob und welche Dark Patterns mit Normen kollidieren, ist eine andere Frage (s. dazu u. II.). Die Gestaltungsmacht auszunutzen, haben Dark Patterns mit Allgemeinen Geschäftsbedingungen gemein. Während letztere unmittelbar *Vertragsbestandteil* werden, wirken Dark Patterns, indem sie die Gestaltungsmacht des Anbieters in der Phase der *Vertragsanbahnung* ausnutzen.

[36] Bei einer möglichen Regulierung könnte es dem Verwender obliegen, die Missbräuchlichkeit zu widerlegen.

[37] Vgl. auch den Rechtsgedanken des § 305c Abs. 1 BGB.

[38] *Bogenstahl* (o. Fn. 10), S. 1: „darauf ausgelegt sind"; *Bösch/Erb et al.,* PPET 2016, 237: „intentionally"; *Greenberg/Boring et al.*, in: Wakkary (Hrsg.), DIS '14, 2014, S. 524: „intentionally".

[39] So auch Sec. 3 lit. a Nr. 1 lit. A DETOUR Act: „with the purpose *or* substantial effect"; iErg ebenso *Rieger*/*Sinders*, Dark Patterns, 13.5.2020, S. 17.

[40] *Weinzierl* NVwZ-Extra 15/2020, 1 (6) zum Schutz von Entscheidungsarchitekturen.

vatautonomie sowie die Berufsfreiheit (Art. 2 Abs. 1 und Art. 12 GG; Art. 15 Abs. 1 GRCh bzw. die unternehmerische Freiheit, Art. 16 GRCh) und die Meinungsfreiheit (Art. 5 Abs. 1 GG; Art. 11 GRCh) ihrer Verwender zu respektieren. Gesetzliche Begrenzungen bedürfen daher einer grundrechtlichen Rechtfertigung.

Die Grundrechte der Nutzer, allen voran deren Vertragsfreiheit, können aber ein legitimes Schutzziel, uU sogar eine Schutzpflicht des Staates begründen, derartige Praktiken zu unterbinden. Denn der Staat hat die Voraussetzungen autonomer Entscheidungen im Geschäftsverkehr aktiv zu sichern.[41] Er ist aufgerufen, die Bedingungen freier Selbstbestimmung mit Hilfe seiner Regelungsmacht tatsächlich herzustellen.

Daraus können zwei konkrete Pflichten erwachsen: Der *Gesetzgeber* ist aufgerufen, sich schützend vor Betroffene zu stellen und das Untermaßverbot nicht zu verletzen. Die *Behörden* und *Gerichte* müssen bestehendes Recht im Sinne dieses Schutzauftrags auslegen und anwenden. Diese Pflicht ist insbesondere dort von besonderer Bedeutung, wo bestehenden Normen ein zu idealisiertes Leitbild des menschlichen Entscheidens zugrunde liegt.

2. Datenschutzrecht

Da Dark Patterns vorwiegend ein digitales Phänomen sind,[42] verwundert es nicht, dass sie häufig einen Bezug zu Datenverarbeitungen aufweisen. Insbesondere bei Gestaltungsmustern für Einwilligungserklärungen zur Datenverarbeitung finden sie sich in reicher Zahl. Ihre steuernde Wirkung kann mit den Vorgaben der DSGVO kollidieren.

a) Wirksamkeit von Einwilligungen

aa) Eindeutig bestätigende Handlung

Einwilligungen bedürfen einer „unmissverständlich abgegebene[n] Willensbekundung […] oder […] sonstigen […] bestätigenden Handlung" (Art. 4 Nr. 11 iVm Art. 6 Abs. 1 UAbs. 1 lit. a DSGVO[43]). Zu diesem Gebot stehen jedenfalls *Opt-out*-Gestaltungen, mithin *Preselection*-Patterns, im Widerspruch (Erwgr. 32 S. 3 DSGVO). Ein Anbieter darf bspw. in der Eingabemaske für ein Online-Gewinnspiel nicht standardmäßig davon ausgehen, dass die Teilnehmenden Werbe-Cookies zustimmen.[44]

Zweifel an einer eindeutig bestätigenden Handlung können auch *Trick Question*- und *Misdirection*-Patterns auslösen, die kontraintuitiv zu ihrer tatsächlichen Funktio-

[41] Vgl. hierzu BVerfGE 81, 242 (254 ff.) = NJW 1990, 1469 (1470); *BVerfG* NJW 2020, 905 (Rn. 231 ff.).

[42] S. o. I. 2.

[43] Diese gelten per Verweis in der ePrivacy-RL etwa auch für den besonders praxisnahen Fall von *Cookies*. Art. 5 Abs. 3 iVm Art. 2 S. 2 lit. f ePrivacy-RL verweist insoweit via Art. 2 Abs. 2 lit. h, Erwgr. 17 S. 1 ePrivacy-RL, Art. 94 Abs. 2 S. 1 DSGVO auf die Vorschriften der DSGVO, s. *BGH* NJW 2020, 2540 (Rn. 29 ff., 60 ff.); *GA Szpunar,* ECLI:EU:C:2019:246 = BeckRS 2019, 3909, Rn. 50 ff. In § 15 Abs. 3 TMG ist mit Blick auf Art. 5 Abs. 3 ePrivacy-RL richtlinienkonform ein Einwilligungserfordernis hineinzulesen, *BGH* NJW 2020, 2540 (Rn. 47 ff.). Klarstellend: § 22 Entwurf eines Gesetzes über den Datenschutz und den Schutz der Privatsphäre in der Telekommunikation und bei Telemedien sowie zur Änderung des Telemediengesetzes (TTDSG-E), 12.1.2020, abrufbar unter https://www.bmwi.de/Redaktion/DE/Downloads/P-R/referentenentwurf-zum-gesetz-zur-regelung-des-datenschutzes-und-des-schutzes-privatsphaere.pdf.

[44] *EuGH* ECLI:EU:C:2019:801 = MMR 2019, 732 (Rn. 60 ff.); s. a. *BGH* NJW 2020, 2540 (Rn. 64); *Taeger/Schweda* ZD 2020, 124 (126).

nalität gestaltet sind.[45] Ein solcher Effekt tritt bspw. ein, wenn ein Anbieter für Auswahlmöglichkeiten in einem Bestellvorgang regelmäßig einen grünen Schiebe-Schalter verwendet, die Datenverarbeitungseinwilligung jedoch als erteilt gelten soll, wenn der Schalter in die andere Richtung weist.

Ob und in welchem Umfang das Vertrauen der Nutzer in die Stringenz von Bedienoberflächen (gerade zwischen verschiedenen Anbietern) in diesen Fällen geschützt ist, verrät der Gesetzeswortlaut nicht. Auch die (nicht mit normativ-autoritativer Macht ausgestatteten) Richtlinien des Europäischen Datenschutzausschusses lassen insoweit eine Konkretisierung vermissen; sie verlangen lediglich, Mehrdeutigkeit bei Einwilligungsgestaltungen zu vermeiden.[46] Damit bleibt die Anforderung der eindeutig bestätigenden Handlung derzeit zu abstrakt, um irreführenden Dark Patterns eine echte Hürde entgegenzusetzen.[47]

bb) Freiwilligkeit

Erklärungen, die ein Anbieter durch starke Täuschung oder Drohung mit erheblichen negativen Wirkungen erreicht, sind nicht von der Autonomie des Einwilligenden getragen und deshalb unfreiwillig.[48] Eine konkrete Ausformung dieser normativen Wertung ist das sog. vertikale Kopplungsverbot: Macht der Anbieter die Vertragserfüllung von einer Einwilligung in die Verarbeitung von Daten abhängig, die zu diesem Zweck gar nicht erforderlich ist, stellt das die Freiwilligkeit einer Einwilligung infrage (Art. 7 Abs. 4 DSGVO). Konditionale Patterns aus der Kategorie „operativer Zwang", die etwa eine Verarbeitungsberechtigung dafür ‚einfordern', dass Nutzer ein anderes, inhaltlich unzusammenhängendes Angebot nutzen können, können diesem vertikalen Koppelungsverbot zuwiderlaufen. Das gilt bspw. für eine digitale Bildbearbeitungssoftware, die Nutzern abverlangt, die Standortverfolgung und -speicherung zu aktivieren.[49]

Weniger eindeutig liegt es bei Dark Patterns solcher Kategorien, die aufgrund ihrer subtileren Wirkungsweise die Schwelle der Unfreiwilligkeit nicht derart eindeutig erreichen, etwa dem *Nagging*-Pattern. Als repetitive Bearbeitungsanfrage kann es – gerade, wenn es optisch aggressiv gestaltet ist[50] – den Eindruck erwecken, dass Datenverarbeitungsrechte zu erteilen sind, bevor jemand eine andere, nicht damit im Zusammenhang stehende Anwendung nutzen kann – auch wenn dies objektiv nicht der Fall ist. Ähnlich gelagert sind *Click Fatigue-Patterns*, die etwa die Verweigerung der Einwilligung von weiteren, umständlichen Handlungen abhängig machen.[51] Sie können

[45] Häufig für Cookie-Einwilligungsfelder genutzt. Beratungsunternehmen empfehlen derartige Konstruktionen explizit, vgl. nur *SUCHMEISTEREI GmbH*, Cookie-Consent mit dem Google Tag Manager, 5.8.2020, S. 7.

[46] *European Data Protection Board*, Guidelines 05/2020 on consent under Regulation 2016/679, 4.5.2020, S. 19.

[47] Auch das Einwilligungsbewusstsein ist derzeit allenfalls als Untergrenze heranzuziehen; *Buchner/Kühling*, in: dies. (Hrsg.), DSGVO mit BDSG, 3. Aufl. 2020, Art. 7 DSGVO Rn. 56.

[48] *European Data Protection Board* (o. Fn. 46), S. 9. Der Zwang bezieht sich auf den Inhalt der Erklärung, nicht auf den Umstand, dass eine Erklärung ergehen muss; s. a. *Martini/Weinzierl* RW 2019, 287 (308 f.).

[49] Bsp. aus *European Data Protection Board* (o. Fn. 46), S. 8.

[50] Etwa indem (iVm einer *Misdirection*) eine Meldung nur einen großen, farblich unterlegten und zentral positionierten „Zustimmen"-Button sowie ein sehr kleines, graues Kreuzchen bereithält, um die Aufforderung zu schließen, und bis zu einer Interaktion die weitere Nutzung verhindert.

[51] Dazu das – nicht-digitale – Bsp. *EuGH* ECLI:EU:C:2020:901 = BeckRS 2020, 30027: Ein Anbieter erbat bei Vertragsabschluss die Einwilligung, eine Personalausweiskopie zu speichern, ohne

eine Einwilligung kraft ihrer subjektiven Wirkung unfreiwillig machen, weil sie eine „echte oder freie Wahl" verhindern (Erwgr. 42 S. 5 DSGVO).

Wenn Nutzer einzelne Bearbeitungszwecke nicht aus- oder abwählen können, mündet das in eine Coactus-volui-Situation: Solche (quasi-)globalen Einwilligungen zur Datensammlung und -verarbeitung verstoßen gegen das sog. *horizontale Koppelungsverbot* (Art. 7 Abs. 2 S. 1, Erwgr. 43 S. 2 1. Hs. DSGVO).[52]

cc) Informiertheit

Zur *Form,* in der der Verantwortliche Informationen zu geben hat, hält die DSGVO (abgesehen von Art. 7 Abs. 2) kaum explizite Vorgaben vor.[53] Der Unionsgesetzgeber hat damit einen eindimensionalen Ansatz gewählt: Er trifft vorwiegend Informationsvorgaben, klammert aber solche mentalen Abweichungen und Limitationen bei der Informationsverarbeitung aus, auf die Dark Patterns aufsatteln. So setzen *Hidden Information*-Patterns darauf, durch ihre optische Gestaltung Nutzer darüber im Unklaren zu belassen, welche Berechtigungen Anbieter konkret erfragen – etwa indem sie Optionen ausblenden. *Trick Questions*-Patterns können durch ihre Formulierung oder überkomplexe Strukturen Verwirrung über den Umfang von Datenverarbeitungen stiften.[54]

Die Rechtsprechung sucht Wege, um solche verhaltenssteuernden Phänomene zu erfassen. Zielt die konkrete Gestaltung der Bedienoberfläche mit Hilfe einer Vielzahl von Auswahlmöglichkeiten darauf ab, dass der Betroffene sich mit ihren Inhalten gar nicht erst auseinandersetzt, sieht der BGH darin keine informierte Einwilligung „für den bestimmten Fall" (Art. 4 Nr. 11 DSGVO).[55] Das Gericht erkennt damit im Grundsatz an, dass schlecht aufbereitete oder im Übermaß vorhandene Informationen nicht dem Normzweck gerecht werden. Der Verantwortliche verstößt zudem potenziell gegen seine Informationspflichten (Art. 13 Abs. 2 lit. b, c DSGVO), wenn seine Einwilligungsarchitektur den Eindruck vermittelt, Vertragsabschluss und Datenverarbeitungseinwilligung seien nicht unabhängig voneinander,[56] er eine horizontale Kopplung mithin nur vorspiegelt. Die Vorgaben setzen also solchen Gestaltungen Grenzen, die Informationen allzu offensichtlich verschleiern bzw. die Auswahlmöglichkeiten sehr unübersichtlich gestalten.[57]

---

dass dies erforderlich war, um den Vertrag zu schließen. Wer die Zustimmung versagte, musste ein zusätzliches Formular ausfüllen.

[52] Außerdem darf das Menü nicht so gestaltet sein, dass es Nutzer davon abhält, Entscheidungen zu treffen; *BGH* NJW 2020, 2540 (Rn. 32). S. dazu sogleich, I. 2. a) bb).

[53] *European Data Protection Board* (o. Fn. 46), S. 16 f. Die Pflichten des Art. 12 Abs. 1 DSGVO beziehen sich auf Art. 13 ff. DSGVO, also nicht unmittelbar auf die Einwilligung; vgl. auch *Bäcker*, in: Kühling/Buchner (Hrsg.), DSGVO mit BDSG, 3. Aufl. 2020, Art. 13 DSGVO Rn. 63 ff.

[54] Vgl. zu „in Kenntnis der Sachlage" und „für den konkreten Fall" iSd Art. 2 lit. h Datenschutz-RL: *BGH* NJW 2020, 2540 (Rn. 31 f.).

[55] *BGH* NJW 2020, 2540 (Rn. 36). Insofern ist die Informiertheit „das subjektive Gegenstück zur Bestimmtheit", *Klement*, in: Simitis/Hornung/Spiecker gen. Döhmann (Hrsg.), DSGVO mit BDSG, 2019, Art. 7 DSGVO Rn. 72.

[56] *EuGH* ECLI:EU:C:2020:901 = BeckRS 2020, 30027 (Rn. 49 f.).

[57] So auch *Böhm/Halim* MMR 2020, 651 (655).

b) *Data Protection by Design* (Art. 25 Abs. 1 DSGVO)

Lenkenden Gestaltungsmustern, die mit Hilfe von Voreinstellungen (und damit unter Ausnutzung des sog. *Default*-Effekts[58]) einseitig die Geschäftsinteressen der Anbieter vor den Privatheitsschutz ihrer Kunden setzen, stellt sich Art. 25 *Abs. 2* DSGVO (*Data Protection by Default*) entgegen. Art. 25 *Abs. 1* DSGVO richtet den Blick über Datenschutzverstöße bei einzelnen *Bearbeitungsvorgängen* hinaus auf die Nutzung grundsätzlich mängelbehafteter *Systeme*: Er schwört die Verantwortlichen auf Datenschutz durch Technikgestaltung (*Data Protection by Design*) ein. Sie sollen den Datenschutz*grundsätzen* (Art. 5 DSGVO) ganzheitlich und von Beginn an bei der Technikgestaltung Raum geben und sie dadurch effektiv umsetzen.[59] Diese Verpflichtung des Verantwortlichen konzipiert die DSGVO als Hebel, um mittelbar auch die Entwickler von Datenverarbeitungssystemen an die Datenschutzziele zu binden.[60] Art. 25 Abs. 1 DSGVO wirkt damit in die Tiefe der Datenverarbeitungsstrukturen hinein.

Zur Technikgestaltung gehört im Grundsatz auch das Design der Anwendungsoberflächen. Denn es repräsentiert die oberste Ebene der technischen Architektur, die den mehrschichtigen Prozess der Datenverarbeitung anleitet: Interfacedesign bahnt den Weg, auf dem sich die technische Gestaltung entfaltet, die die Privatheit schützen soll. Der Wortlaut des Art. 25 Abs. 1 DSGVO lässt sich daher durchaus so verstehen, dass er Design-Muster, zB farbliche Hervorhebungen, als Teil der Technikgestaltung erfasst. Dies geht mit der Philosophie des Data Protection by Design-Gebots, Software insgesamt datenschutzfreundlich auszugestalten, Hand in Hand. Sobald Dark Patterns etwa Nutzer dazu verleiten, größere Datenmengen als erforderlich preiszugeben, konfligieren sie grundsätzlich mit dieser Vorgabe:[61] Art. 25 Abs. 1 DSGVO verweist explizit auf den Grundsatz der Datenminimierung aus Art. 5 Abs. 1 lit. c DSGVO. Der Grundsatz von Treu und Glauben (Art. 5 Abs. 1 lit. a Var. 2 DSGVO) gebietet es zudem, Auswahlmöglichkeiten objektiv, neutral und ohne den Einsatz manipulativer Techniken darzustellen.[62]

Allerdings zieht das Data Protection by Design-Prinzip keine klar konturierten Brandmauern für unzulässiges Verhalten ein.[63] Die offene Struktur der Norm trägt ihren Adressaten vielmehr eine Abwägung hinsichtlich der zu ergreifenden Maßnahmen auf. Eine Vielzahl von Variablen, insbesondere der „Stand der Technik", fließen dabei in das Entscheidungskalkül ein.[64] Die Norm ist auf Maßstäbe angewiesen, welche die Grenzen akzeptabler Beeinflussung (ggf. ausgelagert) festschreiben, um vollzugsfähig zu sein. Schon im Lichte des Bestimmtheitsgebots (Art. 49 Abs. 1 S. 1 GRCh) muss mit Blick auf die Bußgeldbewehrung des Verstoßes (Art. 83 Abs. 4 lit. a DSGVO) stets

[58] *Martini*, in: Paal/Pauly (Hrsg.), DSGVO BDSG, 3. Aufl. 2021, Art. 25 DSGVO Rn. 13.

[59] *European Data Protection Board*, Guidelines 4/2019 on Article 25, 2020, S. 6 f.

[60] Dazu Erwgr. 78 S. 4 DSGVO; *Hansen*, in: Simitis/Hornung/Spiecker gen. Döhmann (Hrsg.), DSGVO mit BDSG, 2019, Art. 25 DSGVO Rn. 20 ff.; *Martini*, in: Paal/Pauly (o. Fn. 58), Art. 25 DSGVO Rn. 25 f.

[61] So auch *European Data Protection Board* (o. Fn. 59), S. 18. Vgl. im Weiteren *Baek/Bae et al.,* The Social Science Journal 2014, 523 (528 f.); *Luguri/Strahilevitz* (o. Fn. 10), S. 22 f. sowie *Martini/Weinzierl* RW 2019, 287 (288 f.).

[62] *European Data Protection Board* (o. Fn. 59), S. 18: „No Deception". Zu Recht sah sich der Europäische Datenschutzausschuss im November 2020 zu der Feststellung veranlasst, dass „Dark Patterns […] gegen den Geist von Artikel 25" DSGVO verstoßen, aaO, S. 19; Übersetzung d. Verf.

[63] So auch *Roßnagel* MMR 2020, 222 (227).

[64] *European Data Protection Board* (o. Fn. 59), S. 8 ff.; *Hansen*, in: Simitis/Hornung/Spiecker gen. Döhmann (o. Fn. 60), Art. 25 DSGVO Rn. 36 ff. schlägt insoweit Datenbanken vor, die den „Stand der Technik" abbilden.

vorhersehbar sein, welches Verhalten der Unionsgesetzgeber dem Verantwortlichen abverlangt.[65]

Die Norm erfasst jedenfalls besonders starke Beeinflussungsstrukturen hinreichend klar – bspw. sehr intensive *Nagging*-Patterns, die in sehr kurzen Zeitintervallen Kunden Verarbeitungsberechtigungen abringen. Dieses nutzt die Gestaltungsmacht besonders intensiv aus und ist mit den Prinzipien guten Technikdesigns inkompatibel.[66] Für Gestaltungen von geringerer Intensität – zB leichte *Misdirection*-Patterns, wie grüne Ablehnungs- und rote Zustimmungsschaltflächen – ist die Norm hingegen zu abwägungsoffen und konkretisierungsbedürftig, um unmittelbar als scharfes Schwert zu wirken.

So entpuppt sich Art. 25 Abs. 1 DSGVO im Ergebnis zwar als potenzielle normative Waffe gegen Dark Patterns.[67] Erst durch Konkretisierungen kann sie jedoch zu einem wirkungsvolleren Instrument erwachsen.[68]

c) Zwischenergebnis

Das Datenschutzrecht verbietet bereits de lege lata einige Ausprägungen von Dark Patterns.[69] Es sind aber vorwiegend Einzelformen verhaltenssteuernder Lenkung, etwa vorausgewählte Kästchen oder die Verzerrung von Informationen, die mit seinen Vorgaben konfligieren. Die Spielräume des Gesetzeswortlauts versuchen die Gerichte immer wieder zu nutzen, um auch andere verhaltenslenkende Dynamiken, mithin die Essenz von Dark Patterns, zu adressieren. Diese repräsentieren jedoch einen ganz eigenen Gefahrentyp für die Privatautonomie, den die DSGVO nicht explizit adressiert. Immerhin liefert Art. 25 Abs. 1 DSGVO das grundsätzliche normative Rüstzeug dafür, Designgestaltungsformen zu erfassen, die den Datenschutzgrundsätzen widersprechen. Dieses gilt es zu nutzen und Standards herauszuarbeiten bzw. anhand von Fallbeispielen die Schwelle zu definieren, ab der Verwender missbräuchlich vorgehen, also einseitig ihre Gestaltungsmacht über Oberflächen ausnutzen.

Der Wirkradius der datenschutzrechtlichen Vorschriften unterliegt einer weiteren wichtigen Einschränkung: Sie richten sich grundsätzlich nicht gegen bestimmte Ver-

---

[65] Vgl. etwa *EuGH* ECLI:EU:C:2020:455 = BeckRS 2020, 11912 (Rn. 47 ff.); *Jarass*, GRCh, 4. Aufl. 2021, Art. 49 Rn. 11. Ein gefestigter Forschungsstand kann sich in Zertifizierungen iSd Art. 25 Abs. 3 iVm Art. 42 DSGVO manifestieren.

[66] Sec. 13 CPRA, zur Änderung von Sec. 1798.135 lit. c Nr. 4 Cal. Civil Code (CCPA) schreibt eine Sperrfrist von zwölf Monaten fest, in der Verantwortliche keine Erlaubnis zur Datennutzung anfragen dürfen, sofern Verbraucher diese einmal versagt haben; dazu *Lejeune* ITRB 2021, 13 (14).

[67] *European Data Protection Board* (o. Fn. 59), S. 19.

[68] Den allgemeineren Grundsatz „Privacy by Design" effektiv zu konkretisieren, um Dark Patterns auf Cookie-Einwilligungsfeldern zu vermeiden, scheint außerdem der Entwurf der Europäischen Kommission für eine ePrivacy-VO (S. COM(2017) 10 final [ePrivacy-VO-E]) zu intendieren. Er etabliert die Pflicht, in Browsersoftware eine Funktion einzubauen, die Cookies bzw. Tracking allgemein unterdrücken können (Art. 10 ePrivacy-VO-E). Daneben verpflichtet der Entwurf Anbieter für bestimmte Datenverarbeitungen zu einem „deutlichen Hinweis", „in hervorgehobener Weise", etwa durch „standardisierte Bildsymbole", „um in leicht wahrnehmbarer, verständlicher und klar nachvollziehbarer Form einen aussagekräftigen Überblick über die Erhebung [von Cookies] zu vermitteln", mithin eine Pflicht zu nutzerfreundlicher Designgestaltung und ein Gegenentwurf zu *Misdirection*-Patterns (Art. 8 Abs. 2 ePrivacy-VO-E). Allerdings tendieren die Mitgliedstaaten im Europäischen Rat derweil dazu, diesen Artikel zu streichen, vgl. COD(2020) 9931, S. 76.

[69] Das Recht, eine Einwilligung zu widerrufen (Art. 7 Abs. 3 S. 1 DSGVO), verheißt kaum eine effektive Handhabe gegen Dark Patterns. Denn nach der erteilten Einwilligung (oder Information über andere Verarbeitungsgrundlagen) werden Nutzer idR nicht mit weiteren Konsequenzen ihrer Entscheidung konfrontiert und verspüren typischerweise wenig Anlass dazu, diese zu überdenken – anders als etwa bei gekauften Sachen, bei denen die Übergabe der Kaufsache materialisiert an die Kaufentscheidung erinnert; s. u. II. 3. a) bb).

arbeitungsinhalte, zB bestimmte Vertragsergebnisse: Das Datenschutzrecht soll zwar das Recht auf Schutz personenbezogener Daten verbürgen, dabei aber nicht ein umfassendes Vertragsinhaltsrecht aus der Taufe heben. Dark Patterns, deren Wirkung darin besteht, den Einzelnen zu einem Vertragsabschluss zu bewegen, ohne ihm zugleich mehr Daten als erforderlich abzuringen, vermag das Datenschutzrecht daher grundsätzlich nicht zu greifen.

3. Vertragsrecht

a) Verbrauchervertragsrecht

Für Anbieter kommerzieller (Shopping-)Webseiten[70] sind Dark Patterns ein reizvoller Weg, um die Reichweite oder den Umsatz zu steigern.[71] Sofern die Anbieter dabei mit Verbrauchern in B2C-Geschäften interagieren, setzen ihnen jedoch die Vorschriften des Verbraucherschutzrechts Grenzen. Obgleich deren Vorgaben nicht explizit auf Dark Patterns abzielen, nehmen sie zum Teil doch ähnliche Wirkmechanismen ins Visier.

aa) Transparenz und Information

Das Verbrauchervertragsrecht tritt beeinflussenden Strategien der Verkaufsförderung primär mit Informations- und Transparenzvorgaben entgegen. Es verpflichtet bspw. Unternehmer bei Verbrauchergeschäften, die Gesamtkosten bereits in der Werbephase auszuweisen.[72] Dies soll *Sunk Cost*-Effekte verhindern, die sich etwa *Hidden Costs*-Patterns zunutze machen,[73] indem sie Nutzer erst in einem späten Bestellschritt über zusätzliche Bearbeitungsgebühren oder höhere Lieferkosten informieren.[74] Alle Zahlungspflichten des Verbrauchers, die über die Hauptleistung hinausgehen, sind außerdem explizit vertraglich festzuhalten; im elektronischen Geschäftsverkehr gilt daher – ähnlich wie im Datenschutzrecht[75] – ein *Opt-out*-Verbot (§ 312a Abs. 3 S. 2 BGB[76]).[77] Für einige Bereiche setzen weitergehende spezielle Regelungen Dark Patterns Grenzen; bei Flugbuchungen etwa gilt sogar ein *Opt-in*-Gebot.[78] Gerade *Sneak into Basket*- sowie *Hidden Costs*-, aber auch *Preselection*-Patterns beschränkt das Verbrauchervertragsrecht damit bereits nachhaltig.

---

[70] Vgl. *Mathur/Acar et al.,* PACM HCI 2019, Article 81, 1 (11 f.); mind. 11 % von 11000 überprüften Shopping-Webseiten nutzten textbasierte und automatisiert auswertbare Dark Patterns; die tatsächliche Quote liegt möglicherweise höher.

[71] *Narayanan/Mathur et al.,* acmquere 2020, 67 (75). Vgl. etwa zu *Scarcity*-Patterns *Bundeskartellamt* (o. Fn. 1), S. 106 ff.

[72] § 1 Abs. 1, 2 PAngV; dieser setzt Art. 7 Abs. 1, 2, 4 lit. c UGP-RL um; vgl. auch Erwgr. 39 S. 2 RL (EU) 2019/2161. Über § 3a UWG findet die Norm Eingang ins Lauterkeitsrecht; s. dazu u. II. 4.

[73] *Mathur/Acar et al.,* PACM HCI 2019, Article 81, 1 (13). Sunk Costs sind bereits getätigte (und daher jedenfalls „verlorene") Aufwendungen. Sie können den Einzelnen psychologisch dazu verleiten, länger an einem Vorhaben festzuhalten als rational sinnvoll, um die eigenen Investitionen vor sich selbst zu rechtfertigen.

[74] Vgl. *Wendehorst*, in: Krüger (Hrsg.), MüKoBGB, 8. Aufl. 2019, § 312a Rn. 75.

[75] S. o., I. 2.

[76] Die Vorschrift setzt Art. 22 Verbraucherrechte-RL um.

[77] Darüber hinaus sind einige Nebenkosten (wie unzumutbare Zahlungsmittelentgelte) generell verboten, § 312a Abs. 4 BGB (Art. 19 Verbraucherrechte-RL); s. dazu *OLG Hamburg* GRUR-RS 2020, 33192.

[78] Art. 23 Abs. 1 S. 4 VO (EG) Nr. 1008/2008 (Luftverkehrsdienste-VO); vgl. auch *EuGH* ECLI:EU:C:2020:301 = MMR 2020, 752 (Rn. 16 ff.). Zum Unterschied zwischen *Opt-out-Verbot* und *Opt-in-Gebot* vgl. *Martini/Weinzierl* RW 2019, 287 (295 ff.).

Digitale, entgeltliche[79] B2C-Geschäftsvorgänge muss der Kunde stets mit einer Schaltfläche final bestätigen, die „mit nichts anderem als den Wörtern ‚zahlungspflichtig bestellen' oder einer vergleichbaren Formulierung" versehen ist (§ 312j Abs. 3, 4 BGB)[80]. Diese *Button-Lösung*[81] ist eine gesetzliche Antwort auf die Praxis, kostenlose Abonnements oder Testphasen automatisch kostenpflichtig zu verlängern, ohne diesen Umstand vor Vertragsschluss transparent zu kommunizieren (sog. Abo-Fallen). Wie streng die Rechtsprechung die Vorgaben der Button-Lösung anwendet, illustriert der Fall des Streamingdienstes *Netflix*: Dieser musste die Formulierung „Mitgliedschaft beginnen kostenpflichtig nach Gratismonat" anpassen. Das KG Berlin sah die Gefahr, dass der Passus „Mitgliedschaft beginnen" die Aufmerksamkeit von der einzugehenden Zahlungsverpflichtung ablenkt.[82]

Teil der Button-Lösung ist ebenso die Pflicht, neben der festgelegten Schaltflächengestaltung auch die anderen zentralen Vertragsinhalte übersichtlich vor Vertragsschluss aufzugliedern (§ 312j Abs. 2 BGB iVm Art. 246a Abs. 1 S. 1 Nr. 4 EGBGB[83]),[84] um über den sich anbahnenden Abschluss eines kostenpflichtigen (Dauer-) Schuldverhältnisses zu informieren.[85] Dies beugt jedenfalls faktisch Fällen von *Forced* oder *Hidden Continuity*-Patterns sowie intransparenten, Verbraucher behindernden Preisdarstellungen (*Price Comparison Prevention*-Patterns) vor.[86]

Darüber hinaus adressieren die verbraucherrechtlichen Vorgaben teilweise die Art und Weise, wie erforderliche Informationen bereitzustellen sind („klar und deutlich", „klar und verständlich", § 312j Abs. 1, 2 BGB)[87]. Wie im Datenschutzrecht ergreift die Rechtsprechung dies als Möglichkeit, auch das Design zu berücksichtigen. So hielt der BGH eine Flugbuchungsgestaltung für unzulässig, die eine nicht optierte Reiserücktrittsversicherung erneut durch ein orange unterlegtes Feld mit der Aufschrift „Weiter – Ich möchte abgesichert sein" neben einem nicht farblich unterlegten und in kleinerer

[79] §§ 312, 310 Abs. 3, 13, 14 BGB. „Entgeltlich" ist richtlinienkonform möglichst weit auszulegen; *Wendehorst* NJW 2014, 577 (580).

[80] Art. 8 Abs. 2 S. 2-4 Verbraucherrechte-RL.

[81] BT-Drs. 17/7745, S. 7; *Wendehorst*, in: Krüger (Hrsg.), MüKoBGB, 8. Aufl. 2019, § 312j Rn. 22 ff. Bei einem Verstoß kommt kein Vertrag zustande, § 312j Abs. 4 BGB.

[82] *KG Berlin* GRUR-RR 2020, 273 (274).

[83] Die Vorschrift setzt Art. 8 Abs. 2 S. 1, Art. 6 Abs. 1 lit. e, Abs. 6 Verbraucherrechte-RL um. Für Fernabsatzverträge und außerhalb von Geschäftsräumen geschlossene Geschäfte verweist außerdem § 312d Abs. 1 BGB auf Art. 246a EGBGB; § 312e BGB erklärt solche Nebenkosten für unzulässig, die der Anbieter nicht vorab kommuniziert.

[84] BT-Drs. 17/7745, S. 10 f.; *OLG München* MMR 2019, 249 (249 ff.); *Boos/Bartsch et al.,* CR 2014, 119 (122). S. dazu a. §§ 5a, 5b Referentenentwurf eines Gesetzes zur Stärkung des Verbraucherschutzes im Wettbewerbs- und Gewerberecht (GStVSch-E), 4.11.2020, abrufbar unter: https://www.bmjv.de/SharedDocs/Gesetzgebungsverfahren/DE/Staerkung_Verbraucherschutz_Wettbewerbs-_und_Gewerberecht.html, der noch strengere Informationspflichten vorsieht. Zur Systematik der Informationspflichten s. *Wendehorst*, in: Krüger (Hrsg.), MüKoBGB, 8. Aufl. 2019, § 312d Rn. 1 ff.

[85] Art. 8 Abs. 2 UAbs. 1 Verbraucherrechte-RL; vgl. BT-Drs. 17/7745, S. 6 f. Zudem erschwert diese strikte Gestaltungsvorgabe es, den finalen Bestätigungs-Button mit anderen Inhalten zu verknüpfen und diesen so zugleich als Einwilligungserklärung auszugestalten, um nicht-erforderliche Daten verarbeiten zu dürfen; mit dieser Idee aber *Moos/Rothkegel* MMR 2019, 732 (738). Ein rechtmäßiger Bestell-Button ist unter den normativen Prämissen so schlicht gestaltet, dass sein rechtsbindender Gehalt nicht mit anderen Angaben auf der Schaltfläche um Aufmerksamkeit konkurriert. Er vermag insofern den Kunden verlässlich dafür zu sensibilisieren, dass ein abzuschließendes Rechtsgeschäft mit Kosten verbunden ist.

[86] Vgl. am Bsp. der Transparenzvorgaben der Luftverkehrsdienste-VO etwa *BGH* GRUR 2017, 283 (294).

[87] Vgl. darüber hinaus Art. 23 Abs. 1 S. 4 Luftverkehrsdienste-VO: „auf klare, *transparente* und eindeutige Art und Weise" (Herv. d. Verf.).

Schrift gehaltenen Feld mit der Aufschrift „Weiter ohne Versicherung“ anbot.[88] Das Urteil verdeutlicht zugleich die Herausforderungen, Dark Patterns mit rechtlichen Mitteln wirksam die Stirn zu bieten: Die im konkreten Fall genutzten faktischen *Misdirection*- und *Preselection*-Patterns zielen nicht darauf ab, Verbrauchern *falsche* Informationen zuzuführen. Sie operieren vielmehr auf einer unterschwelligen Ebene, indem sie eine Auswahloption komplizierter ausformen als die andere.[89] Das normative Handlungsbesteck passt insofern nicht gänzlich zum regulierten Objekt.[90]

Informations- bzw. Transparenzmaßnahmen verhindern zudem nicht per se, dass Anbieter ausgewählte Aspekte in prominenter Weise betonen oder die Aufmerksamkeit der Nutzer auf andere Weise bereits so beanspruchen, dass Verbraucher an die Grenzen ihrer kognitiven Informationsverarbeitungskapazitäten gelangen.[91] Selbst die Button-Lösung mit ihren konkreten Gestaltungsvorgaben für den finalen Bildschirm adressiert ausschließlich die Darstellung zusammenfassender Informationen bzw. des Bestell-Buttons (in ihrem Verhältnis zueinander).[92] *Scarcity*-Banner, die durch ablaufende Zeitanzeigen Bestelldruck aufbauen,[93] oder (willkürlich generierte) *Social Proof*-Hinweise, die zusätzliche Kaufanreize setzen,[94] lassen sich bspw. durch Transparenzvorgaben nur bedingt beim Schopf packen. Informationsvorgaben sind nur begrenzt und nur gegen bestimmte Einflüsse auf Nutzer in Stellung zu bringen. Subtilere Arten der Manipulation, welche Dark Patterns häufig nutzen, bringen das normative System daher schnell an seine Grenzen.

bb) Widerrufsrechte

Als eines seiner wichtigsten verbraucherschutzrechtlichen Instrumente installiert der Gesetzgeber Widerrufsrechte (§ 355 BGB). Sie vermögen Dark Patterns zwar nicht vollständig zu neutralisieren. Sie können aber deren Wirkung rückgängig machen, indem sie Verbrauchern den Weg ebnen, sich von einem Vertrag zu lösen, der unter dem Einfluss von Dark Patterns zustande gekommen ist. Vor allem für zwei Vertragstypen etabliert der Gesetzgeber solche Abwicklungsrechte: für Fernabsatzverträge (§§ 312c, 312g Abs. 1 BGB) und für außerhalb von Geschäftsräumen geschlossene Verträge („AGV“, ehemals Haustürgeschäfte; §§ 312b, 312g Abs. 1 BGB).

Die Vorschriften zu *AGV* lassen die Risikosensibilität des Gesetzgebers hinsichtlich starker, situativer Verbraucherbeeinflussung erkennen, die im Kern auch Dark Patterns auszeichnet.[95] Die Vorschriften zu *Fernabsatzverträgen* folgen demgegenüber einem anderen Grundgedanken: Verbraucher sollen die Möglichkeit haben, Leistungen nach

---

[88] *BGH* GRUR 2017, 283 (283 ff.).

[89] Vgl. *KG Berlin* MMR 2016, 608 (609).

[90] Anders in Bezug auf § 4a Abs. 1 UWG (§ 4 Nr. 1 UWG aF): *OLG Frankfurt/M.* GRUR 2015, 400 (400 f.); *OLG Frankfurt/M.* MMR 2015, 591 (592) und u., II. 4.

[91] Zur Grenze der Aufnahmefähigkeit *Hacker* (o. Fn. 19), S. 118 ff. UU schmälern auch die Informationspflichten selbst – entgegen ihrem Ziel – die Verständlichkeit von Geschäftsabschlüssen, *Föhlisch* MMR 2017, 447 (448).

[92] BT-Drs. 17/7745, S. 10 ff; vgl. auch *KG Berlin* GRUR-RR 2020, 273 (274).

[93] Dies ist vor allem auf Reisewebseiten ein beliebtes Mittel; die Darstellungen sind (mutmaßlich) häufig irreführend oder sogar falsch, *Bundeskartellamt* (o. Fn. 1), S. 99 ff.

[94] Hiergegen richtet sich allerdings das Verbot gefälschter oder irreführender Kundenbewertungen der Nr. 23b, 23c im Anhang zu § 3 Abs. 3 GStVSch-E.

[95] Das Widerrufsrecht erlaubt eine Abkehr von Verträgen, die an Orten zustande kamen, an denen üblicherweise nicht mit einem Vertragsschluss zu rechnen ist. Es adressiert Geschäftsgebaren, welches die (Überrumpelungs-)Dynamik einer konkreten Entscheidungsumgebung ausnutzt, um Verbraucher zu einem Vertragsschluss zu bewegen (Erwgr. 21 S. 2 ff. Verbraucherrechte-RL). *Eidenmüller* AcP 2010, 67 (82 f.).

der Lieferung „in natura“[96] zu begutachten, ohne abschließend an den Vertrag gebunden zu sein. Denn Vertragsobjekte leiden bei Fernabsatzgeschäften generell unter einer beschränkten Darstell- und Erfahrbarkeit.[97]

Obgleich das Widerrufsrecht für Fernabsatzgeschäfte nicht speziell gegen (digitale) Beeinflussungsmöglichkeiten wirken soll, kann es beeinflussten Verbrauchern ein wirksames Schutzrecht gegen Dark Patterns an die Hand geben. Das sub specie seiner gesetzlichen Zielrichtung besser passende AGV-Widerrufsrecht steht ihnen demgegenüber regelmäßig nicht offen, da dieses die physische Anwesenheit der Beteiligten voraussetzt (§ 312b Abs. 1 BGB).

Selbst wenn das Gesetz Betroffenen ein Widerrufsrecht zugesteht, heißt das allerdings nicht, dass sie hiervon in praxi tatsächlich Gebrauch machen, um sich von Geschäften loszusagen, die unter dem Einfluss von Dark Patterns zustande gekommen sind. Denn in das Bewusstsein eines Großteils der beeinflussten Personen gelangt die Wirkung subtil implantierter Dark Patterns nur selten.[98] Zudem haben Verbraucher bei einem Widerruf grundsätzlich die Rücksendekosten zu tragen (§ 357 Abs. 6 S. 1 BGB) und schrecken tendenziell davor zurück, gefühlte Verluste in Kauf zu nehmen, wenn der in Aussicht stehende Mehrwert, wie im Fall von Alltagsgeschäften, gering scheint (sog. *Loss Aversion*[99]).

Bestehende Widerrufsrechte bieten also keine passgenaue Antwort auf vertragliche Bindungen, die unter der Wirkmacht von Dark Patterns zustande gekommen sind. Sie lassen die nötige normative Sensibilität für die praktischen Implikationen von Verhaltensbeeinflussungen noch vermissen.

b) Allgemeines Vertragsrecht

Obgleich Dark Patterns zumindest begrifflich eine moderne Schöpfung sind, begegnet ihnen das allgemeine Vertragsrecht mit seinen altbewährten Instrumenten längst zumindest punktuell. Eine der normativen Grenzen markiert § 123 Abs. 1 Alt. 1 BGB: Ein Vertragspartner kann nicht nur Rechtsgeschäfte wegen Täuschung anfechten, zu denen der Geschäftspartner eindeutig *falsche* Angaben gemacht hat. Er kann auch solchen Verträgen die Wirksamkeit nehmen, die aufgrund *irreführender* Informationen zustande kamen.[100] Solange die (konkludente) Täuschung auf aktivem Handeln beruht, reicht es aus, dass die falsch dargestellten Umstände materiellrechtlich lediglich aus der Sicht des Getäuschten vertragserheblich waren.[101] Eine Willenserklärung, die auf den Eintrag in ein Online-Branchenverzeichnis abzielt, ist daher bspw. anfechtbar, wenn der Vertragspartner sie aufgrund eines *Hidden Costs*-Pattern, namentlich eines im „Kleingedruckten“ verborgenen Hinweises über anfallende Kosten, in der fälschli-

[96] *Wendehorst*, in: Krüger (Hrsg.), MüKoBGB, 8. Aufl. 2019, § 312c Rn. 3.

[97] Erwgr. 14 Fernabsatz-RL; *Wendehorst*, in: Krüger (o. Fn. 96), § 312c Rn. 3. Das Widerrufsrecht gleicht also eine Informationsasymmetrie zwischen Unternehmer und Verbraucher aus; *Hacker* (o. Fn. 19), S. 873 f. Vgl. auch *Schmitt*, Das unionsrechtliche Verbraucherleitbild, 2018, S. 389 f.

[98] *Luguri/Strahilevitz* (o. Fn. 10), S. 24 f.; *Susser/Roessler et al.,* Georgetown Law Technology Review 2019, 1 (26). Solange der Unternehmer den Verbraucher nicht (vollständig) über das Widerrufsrecht unterrichtet hat, beginnt die Frist nicht zu laufen (§ 356 Abs. 3 S. 1 BGB). Es erlischt jedoch in jedem Falle nach zwölf Monaten und 14 Tagen (§ 356 Abs. 3 S. 2 BGB).

[99] *Kahneman*, Thinking, Fast and Slow, 2011, S. 283 ff.

[100] *Armbrüster*, in: Säcker/Rixecker/Oetker et al. (Hrsg,), MüKoBGB, 8. Aufl 2018, § 123 Rn. 29.

[101] *BGH* NJW 1991, 1673 (1674); *Armbrüster*, in: Säcker/Rixecker/Oetker et al. (o. Fn. 100), § 123 Rn. 23.

chen Annahme der Kostenfreiheit abgegeben hat.[102] Allerdings trägt der Getäuschte die Beweislast dafür, dass die Täuschung den Vertragsschluss „nach der allgemeinen Lebenserwartung" beeinflusst hat.[103]

Subtil wirkende Dark Patterns wie unwahre *Scarcity*-Patterns als relevante Auswirkungen auf die menschliche Entscheidungsfindung anzuerkennen, versteht sich nicht von selbst. Es wird aber ihrer faktischen Wirkmacht gerecht, in derartigen Dynamiken eine Täuschung iSd § 123 Abs. 1 Alt. 1 BGB zu erkennen. Irreführende oder erschleichende Dark Patterns[104] können bzw. sollten Schuldverhältnisse also grundsätzlich anfechtbar machen. Andere Muster, wie etwa wahre *Social Proof*- oder *Countdown*-Patterns, erfasst § 123 Abs. 1 Alt. 1 BGB hingegen kategorial nicht. Denn diese wirken, ohne Unwahrheiten zu verbreiten.[105]

Wer Dark Patterns einsetzt, verletzt unter Umständen seine vorvertraglichen Wahrheits- und Aufklärungspflichten aus §§ 311 Abs. 2, 241 Abs. 2 BGB und macht sich damit ggf. nach §§ 280 Abs. 1 S. 1, 311 Abs. 2 Nr. 1, 241 Abs. 2 BGB schadensersatzpflichtig. Das kann (als Folge der gesetzlich vorgesehenen Naturalrestitution) zur Aufhebung eines Vertragsverhältnisses führen.[106] Zwar ist die culpa in contrahendo (c.i.c.) bisher vorwiegend in Fällen von Informationsasymmetrien etabliert. Jedoch zeigt sie sich grundsätzlich auch für Fälle von Rationalitätsasymmetrien zwischen Unternehmern und Verbrauchern offen.[107] Ihr (potenzieller) Anwendungsbereich reicht also über denjenigen des § 123 Abs. 1 Alt. 1 BGB hinaus.

4. Lauterkeitsrecht

Das Lauterkeitsrecht schützt nicht nur die Mitbewerber und das Interesse der Allgemeinheit an einem unverfälschten Wettbewerb, sondern auch die Entscheidungsfreiheit der Verbraucher, insbesondere ihre Fähigkeit, eine informierte Entscheidung zu treffen (§ 1 UWG).[108] Diese Entscheidungsfreiheit drohen Dark Patterns zu unterlaufen. Dem Grenzen zu setzen, ist das Lauterkeitsrecht als Instrument prädestiniert.

a) Anwendbarkeit des UWG

Das UWG ist nur auf „geschäftliche Handlung[en]" iSd § 2 Abs. 1 Nr. 1 UWG anwendbar.[109] Der denkbar weite Terminus erfasst sämtliche Maßnahmen, die dem eigenen Geschäftszweck dienen.[110] Er umschließt das Vorfeld und den Nachgang eines kon-

---

[102] Vgl. *AG Miesbach* MMR 2001, 837 (837 f.); *AG Dresden* NJW-RR 2002, 1137 (1138). Dies löst allerdings auch Konflikte mit den Transparenzgeboten des Verbraucherschutzrechts aus, s. o. II. 3. aa).

[103] *BGH* NJW 1995, 2361 (2362); *Asmussen* NJW 2017, 118 (121 f.).

[104] Zu denken ist etwa an *Hidden Subscription*-, *Hidden Information*- oder *Trick Question*-Patterns sowie willkürlich generierte *Social Proof*- oder *Scarcity*-Patterns.

[105] Insofern ebenso *Ebers* MMR 2018, 423 (426).

[106] Zum Verhältnis von Anfechtung und Schadensersatzanspruch aus c.i.c. s. *Armbrüster*, in: Säcker/Rixecker/Oetker et al. (o. Fn. 100), § 123 Rn. 102 ff. mwN.

[107] *Ebers* MMR 2018, 423 (426).

[108] *Sosnitza*, in: Heermann/Schlingloff (Hrsg.), MüKoUWG, 3. Aufl. 2020, § 1 Rn. 27 mit Verweis auf Art. 2 lit. e, k UGP-RL.

[109] *Köhler*, in: Köhler/Bornkamm/Feddersen et al. (Hrsg.), Beck-KK UWG, 39. Aufl. 2020, § 2 Rn. 3.

[110] *Sosnitza*, in: Ohly/Sosnitza (Hrsg.), UWG, 7. Aufl. 2016, § 2 Abs. 1 Nr. 1 Rn. 8. Der Gesetzgeber beabsichtigt allerdings (insbes. zum Schutze „privater Meinungsäußerung" von sog. „Influencern"), den Wortlaut der Norm etwas einzuengen (nun „unmittelbarer", statt „objektiver" Zusammenhang), vgl. GStVSch-E, S. 19. Ob dies an der Auslegung der Norm substanziell etwas ändern

kreten Geschäftsabschlusses, insbesondere die Außendarstellung in Gestalt von Werbung.[111] Das schließt auch die Nutzeroberflächengestaltung einer Webseite oder App ein, die – insbesondere via Werbung – Einnahmen generieren soll, mithin auch den Einsatz von Dark Patterns.

b) Unzulässigkeitstatbestände der „Schwarzen Liste"

Die „Schwarze Liste" des Anhangs zu § 3 Abs. 3 UWG[112] erfasst einige Dark Patterns und schiebt deren Einsatz im geschäftlichen Verkehr damit jedenfalls gegenüber Verbrauchern einen Riegel vor.

Besonders sticht *Nr. 6* der Liste hervor, welche die UGP-RL als *Bait and Switch*-Technik bezeichnet. Der Tatbestand schützt Verbraucher davor, dass der Anbieter eine Nachfrage durch irreführende Angaben gezielt manipulativ umleitet:[113] Er verbietet, eine andere als die beworbene Ware oder Dienstleistung abzusetzen. Auch ein Dark Pattern aus der Kategorie der Irreführung trägt den Namen *Bait and Switch*. Bei diesem führt der Klick auf eine Schaltfläche zu einem anderen als dem üblicherweise erwarteten Ergebnis – etwa indem ein Button durch sein „X"-Design suggeriert, er schließe ein Pop-up-Fenster, stattdessen dem Nutzer aber auf eine unerwartete Seite weiterleitet.[114] Während sich die Nr. 6 des Anhangs nur auf eine sehr spezifische Situation bezieht, ist das *Bait and Switch*-Pattern vielfältiger. Insbesondere beschränkt sich sein manipulatives Umleitungselement nicht auf konkrete „Waren- oder Dienstleistungsangebote". Das Dark Pattern erfasst Nr. 6 daher grds. nicht.

Nr. 7 verbietet unwahre Angaben über die begrenzte Verfügbarkeit von Waren oder Dienstleistungen. Die Vorschrift soll Geschäftspartner vor Entscheidungsdruck schützen, der in möglicherweise unüberlegte Kaufentscheidungen mündet.[115] Dies kann insbesondere *Scarcity*-Patterns Grenzen setzen, die genau diesen Entscheidungsdruck aufbauen. In Gestalt graphisch hervorgehobener Hinweisflächen suggeriert dieses Pattern auf Buchungs- oder Bestellplattformen eine knappe Verfügbarkeit. Der Wirkradius der Nr. 7 unterliegt jedoch einer wichtigen Schranke: Er zielt auf „unwahre", dh objektiv unrichtige Angaben,[116] operiert also in einer Richtig/falsch-Binarität. *Scarcity*-Patterns können diesen Richtig/falsch-Bereich schnell verlassen, etwa durch frei gesetzte Countdowns oder graphische Gestaltungen. Ist ein Gegenstand im virtuellen Warenkorb tatsächlich nur für 15 Minuten reserviert, mag dies zwar willkürlich, aber trotzdem wahr sein.[117] Nicht eindeutig falsch ist etwa die Angabe „*n* Nutzer sehen sich das gerade an"[118], auch wenn sich diese auf das begutachtete Hotel generell und nicht kon-

---

wird, erscheint jedoch zweifelhaft. Denn die Änderung übernimmt lediglich den Wortlaut des (für die Auslegung ohnehin bereits maßgeblichen) Art. 2 lit. d UGP-RL.

[111] *Bähr*, in: Heermann/Schlingloff (Hrsg.), MüKoUWG, 3. Aufl. 2020, § 2 Rn. 121 ff. Vgl. Art. 1 lit. d UGP-RL.

[112] Er entstammt dem weitgehend wortgleichen Anhang I der UGP-RL.

[113] *Obergfell*, in: Fezer/Büscher/Obergfell (Hrsg.), UWG, 3. Aufl. 2016, Anhang zu § 3 Abs. 3 Nr. 6 Rn. 4.

[114] *Gray/Kou et al.,* CHI 2018, Paper 534, 1 (6 f.).

[115] *Köhler*, in: Köhler/Bornkamm/Feddersen et al. (Hrsg.), Beck-KK UWG, 39. Aufl. 2020, Anhang zu § 3 Abs. 3 Rn. 7.6.

[116] Ob die Behauptung ausdrücklich erfolgen muss, ist str.; dafür: *Köhler*, in: Köhler/Bornkamm/Feddersen et al. (o. Fn. 115), Anhang zu § 3 Abs. 3 Rn. 7.3; aA (auch konkludente Behauptungen werden erfasst) *Sosnitza*, in: Ohly/Sosnitza (Hrsg.), UWG, 7. Aufl. 2016, Anhang (zu § 3 Abs. 3) Rn. 25.

[117] Vgl. *Bundeskartellamt* (o. Fn. 1), S. 107 f. Teilweise nehmen derartige Hinweise auf Vergleichsportalen die Hälfte der Bildschirmanzeige ein.

[118] *Bundeskartellamt* (o. Fn. 1), S. 107.

kret im angegebenen Buchungszeitraum bezieht. Die Muster wirken dann nicht durch eine Täuschung, sondern durch eine emotionale oder auf Biases und Heuristiken zielende Steuerung. Deren Wirkungsweise vermag Nr. 7 nicht zu erfassen.

Misdirection-Patterns können gegen die Verbote aus *Nr. 8* (Sprachenwechsel[119]) verstoßen, *Hidden Costs*-Patterns gegen *Nr. 21* (kostenpflichtige Gratisleistungen) und *Sneaking*-Patterns gegen *Nr. 22* (Täuschung über abgegebene Bestellungen). Die UGP-Änderungs-RL[120] nimmt zudem das Verbot gezielt gefälschter sowie als authentisch präsentierter, aber ungeprüfter Verbraucherbewertungen[121] (Fälle des *Social Proof*-Patterns) sowie verdeckte Werbung in Online-Suchergebnissen (*Disguised Ads*-Pattern) in die Schwarze Liste auf.[122]

Gleichwohl zeigt sich, dass die Schwarze Liste des UWG Dark Patterns nicht systematisch erfasst. Gerade Nr. 6 und Nr. 7 machen den Grund dafür beispielhaft deutlich: Ihren Verboten unterfallen verhaltenssteuernde Wirkungsweisen nicht generell, sondern alleine einzelne Ausprägungen.

c) Verbotstatbestände der §§ 4 ff. UWG

Innerhalb der Verbotstatbestände der §§ 4 ff. UWG öffnen insbesondere die verbraucherschützenden §§ 4a, 5, 5a und 7 UWG Einfallstore für Verbote von Dark Patterns.

§ 4a Abs. 1 S. 1 UWG verbietet „aggressive geschäftliche Handlungen", die den Betroffenen zu geschäftlichen Entscheidungen[123] veranlassen, welche er „andernfalls

---

[119] Vgl. die Bezeichnungen der einzelnen Nrn. entnommen aus *Sosnitza*, in: Ohly/Sosnitza (o. Fn. 116), Anhang (zu § 3 Abs. 3) Rn. 7 ff.

[120] RL (EU) 2019/2161, Art. 3 Abs. 7. lit. a, b.

[121] Dazu sollen bereits „Likes" gehören; Erwgr. 49 RL (EU) 2019/2161 (UGP-Änderungs-RL).

[122] Vgl. Art. 1 Nr. 9 GStVSch-E: neue Nrn. 11, 23b u. 23c Anhang zu § 3 Abs. 3 UWG.

[123] Der Begriff (legaldefiniert in § 2 Abs. 1 Nr. 9 UWG) markiert das Pendant zu der „geschäftlichen Handlung" iSd § 2 Abs. 1 Nr. 1 UWG auf Seiten der Verbraucher bzw. sonstigen Marktteilnehmer (*Bähr*, in: Heermann/Schlingloff [o. Fn. 111], § 2 UWG Rn. 362). „Geschäftlich" iSd Norm ist die Entscheidung schon dann, wenn sie mit dem (potenziellen) Abschluss von „Geschäften" bzw. der Ausübung von vertraglichen Rechten in Zusammenhang steht. Dies umschließt rechtsgeschäftliche Handlungen und vorbereitende Realakte, wie das Betreten eines Geschäfts oder das Aufrufen eines kommerziellen Online-Portals (*BGH* GRUR 2016, 1073 [Rn. 34]; *BGH* GRUR 2017, 1269 [Rn. 19]). Das Entscheidungsverhalten der Nutzer, welches Dark Patterns in der digitalen Welt beeinflussen, ist idR eine solche geschäftliche Entscheidung. Weniger eindeutig zu beantworten ist hingegen, ob ein Verbraucherverhalten nur dann „geschäftlich" ist, wenn die bereitgestellten Leistungen entgeltlich sind bzw. sie sich durch potenzielle geldwerte Veränderungen im Vermögen eines Verbrauchers auswirken (*Köhler*, in: Köhler/Bornkamm/Feddersen et al. [o. Fn. 109], § 2 Rn. 156a; aA *Omsels,* WRP 2016, 553, [559])). Bedeutsam ist diese Frage insbesondere mit Blick auf Online-Leistungen, die (vermeintlich) kostenlos erscheinen. Jedenfalls aus der Möglichkeit, kostenpflichtige Zusatzangebote zu buchen, erwächst eine (potenzielle) entgeltliche Vertragsbeziehung (*Köhler*, in: Köhler/Bornkamm/Feddersen et al. [o. Fn. 109], § 2 Rn. 156a). Dies betrifft zB Premium-Accounts oder hinter einer Paywall verdeckte Zeitungsartikel; selbst der Aufruf zum „Spenden" dürfte darunter fallen. Werbung bloß zur Kenntnis zu nehmen, begründet hingegen noch keine „geschäftliche Entscheidung" (*BGH* GRUR 2015, 698 [Rn. 20]). Doch wenn Nutzer mit ihren persönlichen Daten (insbesondere via Cookies oder anderweitige Tracking-Technologien zur personalisierten Werbung) „bezahlen" (können) – folglich ein dreiseitiger Markt besteht – liegt „Geschäftlichkeit" vor (vgl. *Köhler*, in: Köhler/Bornkamm/Feddersen et al. [o. Fn. 109], § 2 Rn. 159): Die eigenen Daten sind den „wirtschaftlichen Interessen der Verbraucher" iSd Art. 1 UGP-Richtlinie zuzurechnen. Schließlich zeichnen sie sich aus Unternehmenssicht durch einen substanziellen wirtschaftlichen Wert aus (vgl. *Mischau,* ZEuP 2020, 335 [337 f.]). Die Entscheidung der Nutzer, diese Daten preiszugeben, ist das marktbezogene Pendant (vgl. *Omsels* WRP 2016, 553 [556 f.]) zur geschäftlichen Handlung der Verwender, Werbe-Tracking einzusetzen – ebenso wie es eine geschäftliche Entscheidung der Nutzer darstellt, persönliche Daten, wie zB die E-Mail-Adresse, im Rahmen von Gewinnspielen zu überlassen (so *Bähr*, in:

nicht getroffen hätte“. Dies kommt der herkömmlichen Definition von Dark Patterns sehr nahe.

Insbesondere Belästigungen, Nötigungen und unzulässige Beeinflussungen beeinträchtigen „die Entscheidungsfreiheit“ iSd Norm (§ 4a Abs. 1 S. 2 UWG). Solche Kategorien von Dark Patterns, die den Nutzer unter Druck setzen (insb. *Nagging*-Patterns), lassen sich als „Belästigung“ einordnen. Die Tatbestände der „unzumutbaren Belästigungen“ (§ 7 UWG), die vor allem auf Werbung abzielen, können weitere Konstellationen von *Nagging*- oder *Obstruction*-Patterns erfassen. Gerade solche Ausgestaltungen, die in Gestalt von Pop-ups oder „Interstitials“[124] den Bildschirm des Nutzers entweder einnehmen oder ihn zum Wegklicken nötigen, können unzumutbar sein. Jedenfalls gilt dies für Pop-ups ohne Schließmöglichkeit.[125] Für spezifische Arten von Werbung erfordert § 7 Abs. 2 Nr. 2, 3 UWG zudem eine „ausdrückliche Einwilligung“, für die dieselben Grundsätze wie unter Art. 7 DSGVO gelten.[126] Dark Patterns, die auf operativen Zwang setzen, lassen sich im Extremfall als „Nötigung“ (§ 4a Abs. 1 S. 2 Nr. 2 UWG) und solche der Kategorie „Irreführen“ als „unzulässige Beeinflussung“ (§ 4a Abs. 1 S. 2 Nr. 3, S. 3 UWG) qualifizieren.

§ 4a Abs. 1 S. 1, 2 UWG setzt jedoch voraus, dass die aggressive Handlung *erheblich* ist. Die Erheblichkeit bemisst sich nach den Kriterien des Abs. 2. Nicht jede Art von Dark Patterns überschreitet diese Schwelle. „Hindernis“-Patterns, wie das *Roach Motel*-Pattern, gehen gleichwohl im Regelbeispiel des § 4a Abs. 2 Nr. 4 UWG auf: Er adressiert „belastende oder unverhältnismäßige Hindernisse nichtvertraglicher Art“, die den Einzelnen davon abhalten, ihm zustehende vertragliche Rechte auszuüben.

§§ 5, 5a UWG können insbesondere Dark Patterns der Kategorien „Erschleichen“ oder „Irreführen“ erfassen. Ebenso wie § 4a Abs. 1 S. 1 UWG rekurriert § 5 Abs. 1 S. 1 UWG auf geschäftliche Entscheidungen des Betroffenen, die er „andernfalls nicht getroffen hätte“. Während die Informations- und Transparenzpflichten des Verbrauchervertragsrechts den Fokus primär auf den *Inhalt* der erforderlichen Informationen sowie deren Bereitstellung richten,[127] gehen §§ 5, 5a UWG darüber hinaus: Ihre Terminologie („Irreführung“, „Täuschung“) erfasst Praktiken, welche die *Informationsverarbeitung* gezielt manipulieren oder erschweren.[128] Das gilt insbesondere – mit Blick auf Dark Patterns – für die 2. Alt. des § 5 Abs. 1 S. 2 UWG: „sonstige zur Täuschung geeigneten Angaben“. Sie verlässt die Richtig/falsch-Binarität und kann damit den subtilen Wirkmechanismen vieler Dark Patterns womöglich die Stirn bieten.[129] So kann § 5

Heermann/Schlingloff [o. Fn. 111], § 2 UWG Rn. 381; Köhler, in: Köhler/Bornkamm/Feddersen et al. [o. Fn. 109], § 2 Rn. 159). Keine „geschäftlichen Entscheidungen“ sind allenfalls Nutzerverhaltensweisen auf nicht-kommerziellen Plattformen oder Webseiten, die sich ausschließlich durch nicht-personalisierte Werbung finanzieren. Reagiert der Nutzer jedoch aktiv auf die (nicht-personalisierte) Werbung, etwa per Klick auf den Werbe-Link, ist dies wiederum – anders als der bloße Konsum der sonstigen Website-Inhalte – eine geschäftliche Entscheidung.

[124] *Interstitials* öffnen anders als Pop-ups kein neues Fenster, sondern überblenden den eigentlichen Seiteninhalt einer Website für einen gewissen Zeitraum mit Werbung.

[125] Teilweise hält die Lit. Pop-ups unabhängig von einer Schließmöglichkeit generell für wettbewerbswidrig; So *Mankowski*, in: Fezer/Büscher/Obergfell (Hrsg.), UWG, 3. Aufl. 2016, Wettbewerbsrecht des Internets (S 12) Rn. 149 mwN.

[126] *BGH* NJW 2020, 2540 (Rn. 31). Vgl. o. I. 2. a).

[127] S. o. I. 3. a) aa).

[128] Vgl. etwa *EuGH* ECLI:EU:C:2015:361 = GRUR 2015, 701 (702); *LG München I* MMR 2016, 257 (259 f.).

[129] Der BGH stuft eine geschäftliche Handlung iSv § 5 Abs. 1 UWG dann als irreführend ein, wenn das Verständnis, das sie bei den Verkehrskreisen, die sie adressiert, erweckt, mit den tatsächlichen Verhältnissen nicht übereinstimmt, s. *BGH* GRUR 2016, 1193 (Rn. 20); *BGH* GRUR 2018, 1263

Abs. 1 S. 2 Nr. 1 UWG („wesentlichen Merkmale der Ware oder Dienstleistung wie Verfügbarkeit") im Gegensatz zu Nr. 7 der Schwarzen Liste (die nur „unwahre Angaben" betrifft) Formen von *Scarcity*-Patterns erfassen, welche eine knappe Verfügbarkeit von Leistungen nicht behaupten, sondern lediglich suggerieren – zB durch einen Countdown, der gar nicht erklärt, was nach Ablauf der Zeit geschieht. Die Art und Weise der Preisberechnung (§ 5 Abs. 1 S. 2 Nr. 2 UWG) können die „erschleichenden" Dark Patterns, wie *Sneaking*- oder *Hidden Costs*-Patterns, betreffen. Zudem bietet Online-Shopping technische Möglichkeiten, mit Hilfe getrackter Daten für den Nutzer individuelle Preise zu generieren, ohne dass der Nutzer dies erkennen kann. Darauf antwortet der Normgeber bislang lediglich außerhalb des Lauterkeitsrechts mit einer Informationspflicht.[130]

§ 5a Abs. 2 UWG stuft es als unlauter ein, wesentliche Informationen vorzuenthalten. Dem steht es gleich, wesentliche Informationen „in unklarer, unverständlicher oder zweideutiger Weise" bereitzustellen (§ 5a Abs. 2 S. 2 Nr. 2 UWG). Die Vorschrift bietet damit einen Schutzschild gegen irreführende Dark Patterns, wie *Trick Question* oder *Hidden Information*-Patterns. Sie erfasst aber auch die Fälle graphischer *Interface*-Manipulation – etwa wenn der Anbieter Buttons oder Text „versteckt", indem er ihn zB ausgraut, verkleinert oder am Rand platziert.[131] Einen Gesamtpreis nicht zu erwähnen – ein Musterbeispiel des *Sneaking*- oder der *Hidden Costs*-Patterns –, erklärt § 5a Abs. 3 UWG explizit für unzulässig. Flugangebote, die Zusatzkosten für Aufgabegepäck verschweigen, verstoßen gegen § 5a Abs. 2, 4 UWG.[132]

Die UGP/UWG-Novelle statuiert zudem neue Informations- und Transparenzpflichten für die Parameter von Rankingergebnissen in Suchmaschinen sowie die Authentizität von Verbraucherbewertungen.[133] *Social Proof*-Patterns, die zwar authentische, aber selektiv positive Bewertungen platzieren, erfasst die Änderung hingegen nicht.

d) Verbrauchergeneralklausel und Rechtsbruchtatbestand

Neben den speziellen Verbotstatbeständen der §§ 4 ff. UWG wirkt die Verbrauchergeneralklausel des § 3 Abs. 2 UWG als Auffangtatbestand wettbewerbsgefährdenden Steuerungen von Verbrauchern entgegen. Ihre zentrale Tatbestandsvoraussetzung ist neben einem Verstoß gegen die unternehmerische Sorgfalt die „wesentliche Beeinflussung des wirtschaftlichen Verhaltens des Verbrauchers". Maßgeblich ist also – ähnlich wie in §§ 4a Abs. 1 S. 1, 5 Abs. 1 S. 1 UWG und entsprechend der üblichen Definition von Dark Patterns –, dass dessen Entscheidung ohne unternehmerische Einwirkung anders ausge-

(Rn. 11). Entscheidend ist letztlich, dass die (durch das Verbraucherleitbild bestimmte) Verkehrsauffassung und die objektive Realität auseinanderfallen. Auch objektiv zutreffende, aber unklare oder mehrdeutige Angaben können irreführend sein: s. *Ruess*, in: Heermann/Schlingloff (Hrsg.), MüKoUWG, 3. Aufl. 2020, § 5 Rn. 184 ff.

[130] Art. 6 Abs. 1 Verbraucherrechte-RL (geändert durch RL (EU) 2019/2161). Um der unionsrechtlichen Vorgabe Rechnung zu tragen, beabsichtigt die Bundesregierung, Art. 246a EGBGB entsprechend zu ergänzen; s. Entwurf eines Gesetzes zur Änderung des Bürgerlichen Gesetzbuchs und des Einführungsgesetzes zum Bürgerlichen Gesetzbuche in Umsetzung der EU-Richtlinie zur besseren Durchsetzung und Modernisierung der Verbraucherschutzvorschriften der Union und zur Aufhebung der Verordnung zur Übertragung der Zuständigkeit für die Durchführung der Verordnung (EG) Nr. 2006/2004 auf das Bundesministerium der Justiz und für Verbraucherschutz, 13.1.2021, abrufbar unter https://www.bmjv.de/SharedDocs/Gesetzgebungsverfahren/Dokumente/RegE_Bereitstellung digitalerInhalte_2_Modernisierungsrichtlinie.pdf.

[131] Vgl. dazu *LG München I* MMR 2016, 257 (259 f.).

[132] *OLG Dresden* GRUR-RR 2020, 519; s. o., I. 3. a) aa).

[133] Art. 3 RL (EU) 2019/2161; § 5b Abs. 2, 3 UWG nF, vgl. GStVSch-E, S. 30 ff.

fallen wäre. Ob eine Beeinflussung in concreto die Bagatellschwelle der Wesentlichkeit überschreitet, hängt ua von der Häufigkeit, Intensität und Dauer der geschäftlichen Handlung ab.[134] Der weite Wirkradius, den Dark Patterns kraft ihrer örtlichen und zeitlichen Entgrenzung im Internet entfalten, indiziert eine solche Spürbarkeit grundsätzlich.

Der Rechtsbruchtatbestand des § 3a UWG ermöglicht es ferner, mit lauterkeitsrechtlichen Mitteln gegen Rechtsverstöße aus *anderen* Rechtsgebieten, wie Verletzungen berufs-, produkt- oder vertriebsbezogener[135] Normen, vorzugehen.[136] Mit seiner Hilfe können Wettbewerber und Verbraucherschutzorganisationen insbesondere gegen *Hidden Information*- sowie *Hidden Costs*-Dark Patterns intervenieren, die gegen Informationspflichten, etwa aus der PAngV oder der Luftverkehrsdienste-VO[137], aus § 5 TMG oder aus §§ 312a,[138] 312d Abs. 1, 312i BGB[139] verstoßen.[140]

e) Zwischenergebnis

Dark Patterns fallen grundsätzlich in den sachlichen Anwendungsbereich des UWG. Es adressiert diese zwar ebenso wie das sonstige Recht nicht als solche; seine Schwarze Liste wirft vielmehr eher zufällig und ohne phänomenspezifisches Gesamtkonzept Schlaglichter auf einzelne seiner Spielarten. Einige Ansätze des UWG erfassen ihre Wirkprinzipien allerdings zumindest partiell. Dies gilt insbesondere für die Kategorien der Druck ausübenden (über §§ 4a, 7 UWG) sowie der erschleichenden und irreführenden Dark Patterns (über §§ 5, 5a UWG).

Der Schutz der individuellen Entscheidungsautonomie („Entscheidungen", die man ohne einen bestimmten externen Einfluss „nicht getroffen hätte"), durchzieht das UWG wie ein roter Faden.[141] Es schützt zumindest deren *äußere* Komponente, dh die äußere Handlungsfreiheit, indem es Informationspflichten verankert. Viele Dark Patterns greifen jedoch vornehmlich die *innere* Handlungsfreiheit an,[142] indem sie die Art und Weise der Informationswahrnehmung und -verarbeitung manipulieren und dabei verhaltenspsychologische Schwächen ausnutzen. Ob der Unionsgesetzgeber auch den Schutz der inneren Handlungsfreiheit im Blick hatte, ist unklar.[143] In einigen Referenzfällen hat die

---

[134] *Sosnitza*, in: Heermann/Schlingloff (Hrsg.), MüKoUWG, 3. Aufl. 2020, § 3 Rn. 129. Dies bedeutet im Umkehrschluss aber nicht, dass eine unlautere Handlung schon deshalb nicht spürbar ist, weil sie nur einmal oder nur für kurze Zeit vorgenommen worden ist: so *BGH* GRUR 2011, 842 (Rn. 21). Auch nur vereinzelt eingesetzte, dafür aber umso wirkmächtigere Dark Patterns können demnach spürbar sein.

[135] Vgl. die Fallgruppen bei *Ohly*, in: Ohly/Sosnitza (Hrsg.), UWG, 7. Aufl. 2016, § 3a Rn. 31 ff.

[136] Neben einer das Marktverhalten regelnden Tendenz muss der Rechtsverstoß aber im Einzelfall eine *spürbare* Beeinträchtigung der Interessen von Mitbewerbern, Verbrauchern oder sonstigen Marktteilnehmern zur Folge haben. Die Kriterien für eine solche Spürbarkeit entsprechen denen der „Wesentlichkeit" iSd § 3 Abs. 2 UWG. Vgl. *Ohly*, in: Ohly/Sosnitza (o. Fn. 135), § 3a Rn. 30c.

[137] So auch der BGH im Reiserücktrittsversicherungs-Fall (s. o. Fn. 88).

[138] *OLG Hamburg* GRUR-RS 2020, 33192.

[139] *Mankowski*, in: Fezer/Büscher/Obergfell (o. Fn. 125), Wettbewerbsrecht des Internets (S 12), Rn. 182, 205, 223.

[140] Im Anwendungsbereich der UGP-RL dürfte daneben ohnehin § 5a Abs. 2, 4 UWG einschlägig sein. Ob er § 3a UWG sogar verdrängt, darüber gehen die Meinungen auseinander, jedenfalls ist die Norm insoweit richtlinienkonform auszulegen, vgl. *Köhler*, in: Köhler/Bornkamm/Feddersen et al. (Hrsg.), Beck-KK UWG, 39. Aufl. 2020, Vorbemerkungen PAngV Rn. 5; *Ohly*, in: Ohly/Sosnitza (o. Fn. 135), § 3a Rn. 75.

[141] Vgl. §§ 2 Abs. 1 Nr. 8, 4a Abs. 1 S. 1, 5 Abs. 1 S. 1, 5a Abs. 2 Nr. 2, Abs. 6 UWG.

[142] Vgl. zur Abgrenzung von innerer und äußerer Handlungsfreiheit *Micklitz/Namysłowska*, in: Heermann/Schlingloff (Hrsg.), MüKoUWG, 3. Aufl. 2020, UGP-Richtlinie Art. 1 Rn. 9.

[143] Vgl. *Micklitz/Namysłowska*, in: Heermann/Schlingloff (o. Fn. 142), UGP-Richtlinie Art. 1 Rn. 10. Immerhin spricht der Gesetzgeber zB im Rahmen des § 4a UWG mittlerweile von „psychisch

deutsche Rechtsprechung immerhin eine Unlauterkeit mit der mangelhaften *Art und Weise* der Informationsbereitstellung durch Designpraktiken im digitalen Raum begründet.[144] Eine *systematische* Aufarbeitung des internen Entscheidungsfindungsprozesses – und damit der subtilen Wirkmechanismen von Dark Patterns – findet dagegen nicht statt.[145]

5. Sonstige einfachgesetzliche Rechtsmaterien, insbesondere Medienrecht

Neben dem Datenschutz-, Vertrags- und Lauterkeitsrecht berühren Dark Patterns eine Vielzahl weiterer Rechtsbereiche – vom Strafrecht (etwa wegen tatbestandlicher Täuschungshandlung iSd § 263 Abs. 1 StGB durch Abo-Fallen)[146] bis hin zum Recht der Telemedien. Das TMG wird vergleichsweise konkret: Es trägt Diensteanbietern Kennzeichnungspflichten auf, die „leicht erkennbar, unmittelbar erreichbar und ständig verfügbar" ausgestaltet sein müssen (§ 5 Abs. 1). Das ermöglicht es, das Design besonders in den Blick zu nehmen und so *Hidden Information* und *Click Fatigue*-Patterns normativ zu greifen. So hat die Rechtsprechung bereits längere oder verschlungene Klickwege für unzulässig erachtet[147] – ebenso wie eine „kleine, blasse und drucktechnisch nicht hervorgehobene Schrift"[148]. Ähnliche Formulierungen („leicht zugänglich"; „öffentlich und leicht verfügbar"), welche die Informations- und Transparenzpflichten flankieren, verwendet die neue P2B-Verordnung – etwa für die Offenlegung von Ranking-Parametern durch Suchmaschinen oder die Zugänglichkeit eines Beschwerdemanagementsystems.[149] Weitere derartige Vorschriften finden sich im NetzDG („leicht erkennbares, unmittelbar erreichbares und ständig verfügbares Verfahren")[150], im ePrivacy-VO-E („leicht wahrnehmbarer, verständlicher und klar nachvollziehbarer Form", Art. 8 Abs. 3)[151] sowie im Medienstaatsvertrag („leicht wahrnehmbar, unmittelbar erreichbar und ständig verfügbar", §§ 85, 93 Abs. 1 MStV). Der MStV adressiert überdies explizit die nutzerfreundliche Designgestaltung. Er definiert den Begriff der „Benutzeroberfläche" (§ 2 Nr. 15 MStV) und hält Regelungen vor, die Medienangebote (leicht) auffindbar machen sollen. So hat der „in einer Benutzeroberfläche vermittelte Rundfunk in seiner Gesamtheit auf der ersten Auswahlebene unmittelbar erreichbar und leicht auffindbar zu sein" und darf die Auffindbarkeit einzelner Angebote nicht „unbillig behinder[n]" (§ 84 Abs. 3, 2 MStV). Der MStV verfolgt damit allerdings nicht das Ziel, Verbraucher vor verhaltenssteuernden Maßnahmen zu schützen, sondern Medienvielfalt und einen fairen Wettbewerb der Meinungen sicherzustellen.

---

vermittelten Zwang", ohne aber näher auf die psychologischen Wirkmechanismen einzugehen: vgl. GStVSch-E, S. 18 f.

[144] Vgl. *LG Berlin* MMR 2005, 778 (779); *LG München I* MMR 2016, 257 (259 f.).

[145] Vgl. *Omsels* WRP 2016, 553 (Rn. 19).

[146] *BGH* NJW 2014, 2595 (2596 ff.). S. zu Abo-Fallen II. 3. a) aa).

[147] *LG Düsseldorf* MMR 2003, 340; vgl. auch *OLG Düsseldorf* MMR 2014, 393.

[148] *OLG Frankfurt/M.* K&R 2009, 197.

[149] Art. 5 Abs. 2, 10 Abs. 1, 11 Abs. 1 UAbs. 2, Abs. 4 UAbs. 1 VO (EU) 2019/1150 (P2B-VO).

[150] § 3 Abs. 1 NetzDG. Dieses Verfahren soll nach einem Regierungsentwurf in Zukunft zudem „leicht bedienbar" sein, vgl. Entwurf eines Gesetzes zur Änderung des Netzwerkdurchsetzungsgesetzes, 1.4.2020, abrufbar unter: https://www.bmjv.de/DE/Themen/FokusThemen/NetzDG/NetzDG_node.html, S. 3, 48.

[151] COM(2017) 10 final (ePrivacy-VO-E).

III. Herausforderungen bei der Rechtsdurchsetzung

Dark Patterns sind typischerweise sehr subtil konstruiert. So können die Hintergrundgestaltung von Webseiten oder vorsichtig gestaltete beeinflussende Entscheidungsarchitekturen bereits eine erhebliche Wirkung entfalten, ohne Nutzer sonderlich zu irritieren.[152] Das erschwert die Bemühungen, wirksam gegen sie vorzugehen.

Selbst wenn der aufmerksame Nutzer ein unzulässiges Dark Pattern dechiffriert hat, schränken Probleme bei der Beweissicherung nicht selten die Möglichkeiten der Rechtsdurchsetzung ein:[153] Dark Patterns sind oft flüchtig und für den Einzelnen schwer reproduzierbar. Ihre Wirkung ist häufig prozessbezogen und lässt sich dann nicht ohne Weiteres in Bildern einfangen. Beweissichere Methoden erfordern eine hohe technische Kompetenz.[154]

Verbandsklagen nach dem UWG oder UKlaG[155] (bzw. in Zukunft auf Grundlage der neuen Verbandsklage-RL[156]) sowie ggf. der öffentliche Pranger[157] können dieser strukturellen Hilflosigkeit des Einzelnen ein Stück weit abhelfen. Sofern Verbraucherschutzbehörden von Amts wegen tätig werden, ermöglicht die CPC-Verordnung[158] ein koordiniertes, unionsweites Vorgehen. Über diesen Weg erwirkte bspw. die federführende niederländische Datenschutzbehörde gegenüber dem Portal Booking.com, auffällige verbraucherschutzwidrige Praktiken einzustellen[159] – darunter auch (wenngleich nicht als solche bezeichnete) Dark Patterns. Zudem stehen den Aufsichtsbehörden Nachforschungsbefugnisse, wie Auskunftsbegehren, gegenüber den Verantwortlichen zu (Art. 58 Abs. 1 lit. a DSGVO). Auf diese Weise könnten sie (in den Grenzen ihrer datenschutzrechtlichen Kompetenzen) etwa in Erfahrung bringen, ob ein Anbieter Dark Patterns testet oder gar personalisiert. Die novellierte UGP-RL droht Anbietern nun auch höhere, umsatzabhängige Bußgelder an.[160] Sie verlangt zudem einen Zugang zu angemessenen und wirksamen Rechtsbehelfen, einschließlich Schadensersatz.[161] Dies eröffnet Verbrauchern und ihren Schutzorganisationen grundsätzlich einen Weg, um gegen Dark Patterns vorzugehen.

Die Heterogenität der individuellen menschlichen Reaktionsmuster erschwert die Aufgabe der Rechtsdurchsetzung allerdings weiter. Denn Dark Patterns wirken bei Menschen mit verschiedenen Eigenschaften und Hintergründen unterschiedlich und lassen sich angepasst an individuelle Schwächen ausspielen.[162] Platzieren Anbieter ge-

---

[152] *Luguri/Strahilevitz* (o. Fn. 10), S. 24 ff.; *Mandel/Johnson,* J Consum Res 2002, 235 (240 ff.).

[153] Vgl. *Ebers* MMR 2018, 423 (427).

[154] *Mankowski*, in: Fezer/Büscher/Obergfell (o. Fn. 125), Wettbewerbsrecht des Internets (S 12) Rn. 314 ff. Dies gilt umsomehr, als einfache Ausdrucke oder Screenshots von Webseiten sich leicht manipulieren lassen und daher nur eingeschränkte Beweiskraft entfalten.

[155] Dazu *Uebele* GRUR 2019, 694 (697 ff.).

[156] Die RL (EU) 2020/1828 ersetzt die alte Unterlassungsklage-RL (2009/22/EG), vgl. Art. 21. Verbraucher können dadurch über qualifizierte Einrichtungen leichter gegen (grenzüberschreitende) Verstöße gegen verbraucherschützendes Unionsrecht und der DSGVO (vgl. Anhang I der RL). Dazu näher *Augenhofer* NJW 2021, 113.

[157] Etwa https://twitter.com/darkpatterns.

[158] VO (EU) 2017/2394.

[159] MMR-Aktuell 2020, 424225. Weitere Beschwerden wegen Dark Patterns sind bereits anhängig, u.a. gegen Amazon (wegen erschwerter Kündigungsmöglichkeit von Amazon Prime [Roach Motel]) und Google (Standort-Tracking), vgl. *Forbrukerrådet*, Amazon manipulates customers to stay subscribed, 14.1.2021, abrufbar unter: https://www.forbrukerradet.no/news-in-english/amazon-manipulates-customers-to-stay-subscribed/.

[160] Art. 3 Nr. 6 RL (EU) 2019/2161. Vgl. auch Art. 1 Nr. 5, 7 GStVSch-E.

[161] Art. 3 Nr. 5 RL (EU) 2019/2161. Vgl. auch Art. 1 Nr. 5 GStVSch-E.

[162] S. o., I. 1.

zielt personalisierte Inhalte, birgt das insbesondere für Minderheiten oder marginalisierte Gruppen Gefährdungspotenzial.[163] Um wirksam gegen Dark Patterns vorzugehen, ist daher eine besonders hohe Sensibilität hinsichtlich ihrer Wirkweise und Spezifika angezeigt. Eine starke institutionelle Koordination sowie technischer Sachverstand sind hierfür die condicio sine qua non.

IV. Schlussfolgerungen und Ausblick

1. Dark Patterns de lege lata und Regulierungsansätze

Das Phänomen „Dark Patterns" ist seit mehr als einer Dekade bekannt. Weder der deutsche noch der unionale Gesetzgeber sind gegen sie bisher explizit tätig geworden. Nichtsdestotrotz setzt das Recht bereits heute implizit einigen Designmustern Grenzen, mit deren Hilfe Verwender ihre Gestaltungsmacht einseitig zu ihrem Vorteil ausnutzen. Insbesondere das Lauterkeits- und Verbraucherschutzrecht unterbinden diverse Dark Patterns, wie *Hidden Information*, *Preselection*, *Price Comparison Prevention* oder *Hidden Costs*. Dass diese in der internationalen wissenschaftlichen Diskussion über Dark Patterns gleichwohl so viel Aufmerksamkeit erfahren, gründet auch auf die international unterschiedliche Gesetzeslage: In Übersee sind die Schutzlücken größer als in Europa.

Regulierungsbedarf verursacht hierzulande vor allem die Kategorie „(gefühlter) Druck". Denn für *Confirmshaming*- oder *Social Proof*-Patterns ist das gesetzgeberische Bewusstsein bisher nicht besonders ausgeprägt.[164] Ihre Relevanz springt auch nicht unmittelbar ins Auge. Ähnlich wie irreführende Oberflächengestaltungen sind sie zudem ein qualitativ graduelles Phänomen, dem kein pauschaler Verwerflichkeitsgrad anhaftet.

Dass sich das Recht bislang nur punktuell Dark Patterns in den Weg stellt, legt ein strukturelles Regelungsdefizit offen: Das vielerorts vorherrschende Leitbild des informationsbedürftigen und informierbaren Verbrauchers sowie das daran anknüpfende Regulierungskonzept des „Informationsmodells"[165] wirkt häufig als zu enger normativer Flaschenhals für verhaltensökonomische und psychologische Erkenntnisse über menschliche Entscheidungswege.[166] Zwar kann es etwa in Fällen der Preisintransparenz gleichsam als Schutzkorken gegen Dark Patterns wirken, indem es dem Verbraucher die notwendigen Informationen an die Hand gibt.[167] Doch zeigt sich, dass situative Informationen oft nicht dazu in der Lage sind, die Steuerungswirkung konkreter Designelemente zu unterbinden. Das gesetzliche Verbraucherleitbild vernachlässigt insbesondere innere Restriktionen der menschlichen Entscheidungsfindung, die von kognitiven, emotionalen oder situativen Faktoren ausgehen.[168] Dies gilt umso mehr, als solche Einflüsse grundsätzlich nicht nur bei besonders verletzlichen Personengruppen, sondern bei jedermann wirken können.[169] Erfolg versprechende Maßnahmen gegen Dark Patterns müssen den regulativen Fokus deshalb verstärkt auf solche Umstände menschlicher Entscheidungs-

[163] Vgl. *O'Neil*, Weapons of Math Destruction, 2017, S. 66 ff.
[164] Zumindest hinsichtlich unwahrer *Social Proof*-Patterns verspricht aber Nr. 23b, 23c Anhang zu § 3 Abs. 3 GStVSch-E Abhilfe.
[165] S. hierzu *Tamm*, Verbraucherschutzrecht, 2011, S. 150; *Weber,* ZRP 2020, 98.
[166] Vgl. *Weinzierl* NVwZ-Extra 15/2020, 1 (9).
[167] *Micklitz/Rott*, in: Dauses (Hrsg.), Handbuch des EU-Wirtschaftsrechts, 50. Aufl. 2019, Rn. 119.
[168] *Hacker* (o. Fn. 19), S. 432 ff.; *Rischkowsky/Döring,* J Consum Policy 2008, 285 (309); *Schmitt* (o. Fn. 97), S. 548 f.
[169] Vgl. *Weber* ZRP 2020, 98 (101).

findung erweitern sowie die Interpretation bestehender Normen stärker am tatsächlichen menschlichen Verhalten ausrichten.

Das vergleichsweise junge Datenschutzrecht leidet als Schutzinstrument gegen Dark Patterns an vielen Stellen an ähnlichen strukturellen Defiziten wie das Verbraucher- und Wettbewerbsrecht. Das allgemeine Vertragsrecht scheint durch seine am Einzelfall orientierte Perspektive demgegenüber weniger anfällig für pauschalisierende Verbraucherbilder und damit in der Lage, individuelle Entscheidungsschwächen aufzugreifen. Doch löst es diese Erwartung letzten Endes nicht vollständig ein: Fallen Dark Patterns in die Kategorien „irreführend" oder „erschleichend", können Verträge zwar ggf. anfechtbar sein; allerdings harrt diese Auslegung zum einen noch einer Anpassung der Rechtsprechung an verhaltensökonomische sowie psychologische Erkenntnisse. Zum anderen wirken zahlreiche Dark Patterns, ohne Unwahrheiten zu verbreiten (zB mit Hilfe sozialen Drucks).

Den vielversprechendsten Ansatzpunkt für die Maßnahmen gegen Dark Patterns bieten generalklauselartige Tatbestände, wie die c.i.c. im Schuldrecht oder der *Data Protection by Design*-Grundsatz im Datenschutzrecht. An diesen Stellen weist das Gesetz jeweils eine – ausfüllungsfähige und -bedürftige – regulatorische Flexibilität auf. Allerdings haftet dieser generalklauselartigen Struktur notwendig Rechtsunsicherheit an. Jedenfalls für Konstellationen, die im auslegungstechnischen „Graubereich" liegen, sollte der Gesetzgeber daher missbräuchlichen Patterns mit weiteren Spezialregelungen explizit entgegentreten und verhaltensökonomische Erkenntnisse stärker in Gesetzesbegründungen bzw. Erwägungsgründe einfließen lassen.

Anstelle einer „großen Lösung" in Gestalt eines umfassenden Gesetzes, das Verhaltensmanipulation im digitalen Raum ins Visier nimmt, kann der Gesetzgeber mit kleinem Räderwerk gezielt nachsteuern, indem er etwa zusätzliche Typen oder Kategorien von Dark Patterns in die „Schwarze Liste" des UWG bzw. der UGP-RL aufnimmt. Ein gangbarer Weg besteht auch darin, allgemeinere lauterkeitsrechtliche Verbotstatbestände stärker auf die Wirkweisen von Dark Patterns zuzuschneiden. Zudem wären bestehende Informationspflichten oder Beschwerdemanagementsysteme durch explizite Gebote, eine klare und verständliche Art und Weise der Informationsbereitstellung nicht durch irreführende, ablenkende oder unnötigen Aufwand erzeugende Designmethoden zu umgehen, zu flankieren.[170] Im Datenschutzrecht könnte der Gesetzgeber die Anforderungen an eine wirksame Einwilligung nachschärfen. Möglich wäre eine Ergänzung etwa des Art. 7 DSGVO durch ein Erfordernis, dass bei einer Wahlsituation sämtliche Entscheidungsoptionen auch hinsichtlich ihres Designs gleich zu behandeln sind[171] oder in Art. 9 Abs. 2 lit. a DSGVO die Voraussetzung „[ausdrücklich] und ohne steuernden Einfluss".[172]

Richtig ist es zugleich, nicht generell Dark Patterns (etwa jegliche verwirrend formulierte Frage) nach dem Rasenmäherprinzip pauschal für unzulässig zu erklären. Ein wirksamer Schutz vor Dark Patterns sollte sich vielmehr auf die Regulierung solcher Erscheinungsformen begrenzen, die eine kritische Schwelle der Ausnutzung privatautonomer Gestaltungsfreiheit überschreiten. Darüber hinaus sollte der Gesetzgeber bei den Methoden ansetzen, die Dark Patterns ihre besondere Wirkmacht verleihen: der Möglichkeit gezielten Testens. Dass solche Tests zum Einsatz kommen, ließe sich

[170] Vgl. auch *Baumgartner/Hansch,* ZD 2020, 435 (438); *Weinzierl* NVwZ-Extra 15/2020, 1 (10).
[171] Die französische Datenschutzbehörde CNIL fordert dies bereits in Bezug auf Cookie-Banner, s. *Baumgartner/Hansch* ZD 2020, 435 (438).
[172] *Weinzierl* NVwZ-Extra 15/2020, 1 (10).

durch Informationsansprüche gegen Verwender digitaler Oberflächen zumindest transparent machen. Denkbar ist eine Pflicht, die Ergebnisse von A/B-Tests bei berechtigtem Interesse offenzulegen und/oder deren Durchführung betroffenen Nutzern generell kundzutun.[173] Dieses Wissen wäre ein Grundstein, um die bestehende Informations- und Machtasymmetrie zugunsten von Verbrauchern abzutragen. Denkbar sind daneben ergänzende technische Vorkehrungen oder Apps, die Dark Patterns aufdecken oder gar unterdrücken.

2. Abhilfe in Sicht?

Dark Patterns sind im digitalen Raum omnipräsent. Im günstigsten Fall sind sie nur lästig, im schlimmsten Fall untergraben sie sublim und strukturell die Entscheidungsautonomie des Einzelnen. Staatliche Behörden und der Gesetzgeber erkennen die Problematik erst allmählich. Hat die Europäische Union im Bereich des Datenschutzes mit der DSGVO noch weltweit Pionierarbeit geleistet, kommen die ersten legislativen Vorstöße zum Umgang mit Dark Patterns mit dem DETOUR Act sowie dem novellierten California Privacy Rights Act nun aus den USA. Das geplante Telekommunikations-Telemedien-Datenschutz-Gesetz (TTDSG) korrigiert in Bezug auf Cookie-Einwilligungen bisher lediglich die bis dato unzureichende Umsetzung des Art. 5 Abs. 3 e-Privacy-RL im Nachgang der *Planet 49*-Urteile.[174] Die Novelle der UGP-RL[175] beschränkt sich weitgehend auf Informationspflichten und Rankings von Suchergebnissen. Die Digitale-Inhalte-Richtlinie[176] adressiert wiederum vertragliche Rechte in Zusammenhang mit digitalen Produkten, nicht hingegen verhaltenssteuernde Praktiken außerhalb eines Vertragsverhältnisses.

Die Europäische Kommission hat derweil aber ein Legislativpaket vorgelegt, das den europäischen Rechtsrahmen für digitale Dienste (der seit der E-Commerce-RL aus dem Jahre 2000 keine Veränderung erfahren hat) umfassend neu abstecken soll: Der *Digital Services Act* (DSA) adressiert den Umgang mit „illegalen Inhalten" sowie mit Meinungsfreiheit und Falschinformationen auf digitalen Plattformen.[177] Der *Digital Markets Act* (DMA)[178] versucht flankierend, die Marktmacht der Digitalriesen („Torwächterfunktion") zu begrenzen. Der DSA adressiert zwar grundsätzlich auch die Problematik manipulativer Verhaltenssteuerung.[179] Darauf, dass nicht nur Dritte, sondern Facebook und Co. *selbst* flächendeckend mittels Dark Patterns manipulieren, gehen beide Entwürfe – trotz Problembewusstseins der Kommission[180] – bisher nicht direkt ein. Sie verpassen damit eine Chance. Lobenswerte Ansätze finden sich immerhin

[173] Vgl. auch Sec. 3 lit. b DETOUR Act; *Weinzierl* NVwZ-Extra 15/2020, 1.
[174] Vgl. TTDSG-E (s. Fn. 43), S. 31 ff.
[175] S. a. GStVSch-E.
[176] RL (EU) 2019/770; s. a. Entwurf eines Gesetzes zur Umsetzung der Richtlinie über bestimmte vertragsrechtliche Aspekte der Bereitstellung digitaler Inhalte und digitaler Dienstleistungen, 13.1.2021, abrufbar unter: https://www.bmjv.de/SharedDocs/Gesetzgebungsverfahren/DE/Bereitsstellung_digitaler_Inhalte.html.
[177] COM(2020) 825 final, S. 2 ff.
[178] COM(2020) 842 final.
[179] Vgl. Erwgr. 32, 63, 68, Art. 26 Abs. 1 lit. c COM(2020) 825 final.
[180] Vgl. *Ms Jourová on behalf of EU Commission*, Question E-000774/19 to the Commission. Das Europäische Parlament operiert zwar ebenfalls mit dem Begriff, thematisiert das Phänomen im Vorfeld des DSA aber eher am Rande: vgl. *Europäisches Parlament*, REPORT with recommendations to the Commission on the Digital Services Act: Improving the functioning of the Single Market (2020/2018(INL)), 7.10.2020; *Europäisches Parlament, Fachabteilung Wirtschaft, Wissenschaft und Lebensqualität*, New aspects and challenges in consumer protection, April 2020, S. 23, 36.

in Bezug auf die Transparenzpflichten, insbesondere im Zusammenhang mit personalisierter Werbung und Empfehlungsalgorithmen.[181]

Die Gefahren, die von Dark Patterns ausgehen, sollten den europäischen und den nationalen Gesetzgeber sowie die zuständigen Verwaltungen anspornen, nach passgenauen Lösungen zu suchen. Um Dark Patterns gleichsam aus der rechtlichen Dunkelheit zu holen, müssten die zuständigen Entscheidungsträger den regulatorischen Scheinwerfer nicht nur auf Teilphänomene, sondern auf sämtliche Typen und Kategorien, insbesondere gefühlten Druck, richten. Einstweilen bleibt der Eindruck: „[…] die einen sind im Dunkeln und die andern sind im Licht, und man siehet die im Lichte, die im Dunkeln sieht man nicht."[182] Solange diese Grundregel für die manipulative Gestaltung digitaler Oberflächen gilt, tappt jeder verbraucherpolitische Schutzmechanismus gegen Dark Patterns im Dunkeln.

V. Ergebnisse

1. Dark Patterns sind Designmuster, die eine kritische Zahl an Nutzern zu einem bestimmten Verhalten verleiten und dabei die Gestaltungsmacht über Benutzeroberflächen einseitig im Interesse ihrer Verwender ausnutzen.
2. Das Datenschutz- und Verbrauchervertragsrecht verbietet ebenso wie das Lauterkeitsrecht bereits einige Ausprägungen von Dark Patterns; diese lediglich punktuellen Verbote zeigen jedoch eine systemische Schwachstelle auf: Das zugrunde liegende Verbraucherleitbild erkennt die vielfältigen Steuerungsmöglichkeiten nicht.
3. Um bestehende gesetzliche Lücken zu schließen, ist es einerseits nötig, die Auslegungsmethoden an aktuelle verhaltensökonomische und -psychologische Erkenntnisse anzupassen und andererseits explizite Regelungen zu schaffen, die unterschwellige Beeinflussungen abseits der Informationsebene stärker adressieren.

The advancing digitization of commercial interactions creates ever growing possibilities to influence human decision making. So-called "Dark Patterns" allow designers of digital user-interfaces to steer users into taking decisions they would not have made otherwise. Although Dark Patterns constitute a relatively recent development, data protection, consumer protection as well as fair trading law already prohibit some of their manifestations. Nevertheless, these legal regimes are often based on the model of the rational consumer. The subliminal effects of Dark Patterns however reveal the particular risks boundedly-rational actors face. This finding indicates legal adjustments.

[181] Vgl. Art. 24, 29, 30 COM(2020) 825 final.
[182] *Bertolt Brecht*, Dreigroschenoper, Schlussstrophe.