

Ass. iur. Quirin Weinzierl, LL. M. (Yale)\*

## Dark Patterns als Herausforderung für das Recht

### Rechtlicher Schutz vor der Ausnutzung von Verhaltensanomalien

Die Diskussion zu verhaltenswissenschaftlichen Erkenntnissen und Recht (Behavioral Law and Economics) dreht sich um zwei Fragen: die Grenzen des Einsatzes verhaltenswissenschaftlicher Regulierungsinstrumente (Nudging) sowie die Kritik an etablierten Regulierungskonzepten, insbesondere dem Informationsmodell. Dark Patterns rufen eine dritte Frage auf den Plan: der Schutz vor der Ausnutzung von Verhaltensanomalien durch Private. Der Beitrag ordnet dieses neue Phänomen (verhaltens-)ökonomisch sowie rechtlich ein. Er entwickelt Grundlinien zum verfassungsrechtlich erforderlichen Autonomieschutz sowie einer regulatorischen Antwort auf Dark Patterns.

#### I. Dark Patterns als Ausnutzung von Verhaltensanomalien

##### 1. Dark Patterns in der Praxis

In der digitalen Welt finden sich Nutzer regelmäßig in Situationen, in denen sie Einwilligungen und andere Formen der Willenserklärung abgeben sowie sonstige Entscheidungen treffen – von der Zustimmung zu Cookies bis zur Buchung eines Hotels. Dabei sind sie oft mit Entscheidungsumgebungen konfrontiert, die auf ihre Willensbildung Einfluss nehmen oder dies zumindest versuchen. Beispiele sind Voreinstellungen von Eingabemöglichkeiten, Countdowns zur zeitlichen Befristung von Entscheidungen,<sup>1</sup> Verweise auf (vermeintliche) Knappheit und das (vermeintliche<sup>2</sup>) Verhalten anderer Nutzer, farbliche und sonstige graphische Gestaltungen von Benutzeroberflächen, bestimmte Arten, Fragen und Informationen zu präsentieren, oder der Zwang zu entscheiden.<sup>3</sup>

In all diesen Situationen stellt sich bei dem Nutzer das Gefühl ein, der Anbieter steuert ihn, setzt ihn unter Druck und führt ihn gar hinters Licht. Kurz gesagt: Der Nutzer fühlt sich manipuliert. Diese Situationen haben in jüngster Zeit unter dem Schlagwort *Dark Patterns* journalistische,<sup>4</sup> politische<sup>5</sup> und wissenschaftliche Aufmerksamkeit erfahren. Nach der klassischen Definition *Harry Brignull's* beschreibt

der Begriff – aus Perspektive der *User-Interface (UI)-Design-Forschung* – „eine Benutzeroberfläche, die sorgfältig ausgearbeitet wurde, um Benutzer auszutricksen, damit sie Dinge tun, die sie sonst möglicherweise nicht tun würden“.<sup>6</sup>

#### 2. Dark Patterns aus verhaltenswissenschaftlicher Sicht

Um Dark Patterns rechtlich greifbar zu machen, hilft eine Beschreibung aus verhaltenswissenschaftlicher bzw. -öko-

\* Der Verf. ist Forschungsreferent im Programmbereich „Digitalisierung“ am Deutschen Forschungsinstitut für öffentliche Verwaltung, Speyer. Er ist Koordinator des von Professor *Dr. Mario Martini* betreuten BMJV-Forschungsprojekts „Dark-Pattern-Detection-App (DaPDA)“. Der Aufsatz ist als Teil dieses Projekts entstanden. Der Verf. dankt Professorin *Dr. Christiane Schwieren* (Universität Heidelberg) für wertvolle Hinweise sowie stud. iur. *Ulrike Urbanek* für die gelungene Unterstützung.

1 Vgl. *Blenkinsop*, *Booking.com agrees to EU demands to change travel offers*, 20.12.2019, abrufbar im Internet: <https://www.reuters.com/article/us-booking-hldg-eu/booking-com-agrees-to-change-way-it-presents-travel-offers-eu-idUSKBN1YO18C> (Stand: 27.4.2020).

2 *Mathur/Acar et al.*, *Proc. ACM Hum.-Comput. Interact.*, CSCW 2019, Article 81, 18, zu Zahlengeneratoren.

3 Vgl. etwa die Dokumentation von *Norwegian Consumer Council*, *Deceived by Design*, 2018.

4 *Smith*, *Why you can't escape dark patterns*, 7.2.2020, abrufbar im Internet: <https://www.fastcompany.com/90452333/why-you-still-cant-escape-dark-patterns> (Stand: 29.5.2020); *Siebert*, *Abzocke im Internet*, 6.4.2020, abrufbar im Internet: <https://www.bild.de/bild-plus/politik/inland/politik-inland/abzocke-im-internet-wann-online-haendler-zuweit-gehen-69662564,view=conversionToLogin.bild.html> (Stand: 10.4.2020).

5 *Bogenstabl*, *Dark Patterns – Mechanismen (be)trügerischen Internetdesigns*, 2019; *Rieger/Sinders*, *Dark Patterns: Design mit gesellschaftlichen Nebenwirkungen*, 2020; sowie nachfolgende Quellen.

6 *Brignull*, *Dark Patterns: dirty tricks designers use to make people do stuff*, 8.7.2010, abrufbar im Internet: <https://www.90percentofeverything.com/2010/07/08/dark-patterns-dirty-tricks-designers-use-to-make-people-do-stuff/> (Stand: 29.5.2020); Übersetzung des Verf. In diese Richtung *Conti/Sobieski* in *Rappal/Jones et al.*, *ACM WWW '10 Proceedings*, 2010, 271 (271); *Gray/Kou et al.* in *Mandryk/Hancock*, *ACM CHI '18 Proceedings*, 2018, Paper 534, 1; *Nouwens/Liccardi et al.* in *Bernhaupt/Mueller/Verweij*, *ACM CHI '20 Proceedings*, 2020, Paper 194, 3.

nomischer Sicht. Im Gegensatz zur UI-Design-Sichtweise kann diese erklären, *warum* bzw. *wie* Dark Patterns wirken.<sup>7</sup>

a) *Rational Choice Theory und Verhaltensanomalien*. Verhaltensökonomische Erkenntnisse über das Entscheidungsverhalten von Menschen sind nicht neu und sollen deswegen hier nur kurz umrissen werden.<sup>8</sup> Ausgangspunkt ist die neoklassische Ökonomie, welche auf dem Modell rationaler Entscheidungen (*Rational Choice Theory*) basiert.<sup>9</sup> Sie geht davon aus, dass der Mensch – im Rahmen der Gegebenheiten – seinen Nutzen vergrößern will und dabei rational nach einer Kosten-Nutzen-Abwägung entscheidet (sog Erwartungsnutzen-Theorie bzw. *Expected Utility Theory*).<sup>10</sup> Ineffiziente Entscheidungen resultieren hiernach – abgesehen von Fällen des Marktversagens – alleine aus sog Transaktionskosten (*Switching Costs*).<sup>11</sup> Die Rational Choice Theory konzipiert insoweit das Menschenbild des *homo oeconomicus*.<sup>12</sup>

Umfassende verhaltenswissenschaftliche Studien haben gezeigt, dass der Mensch diese Rationalitätserwartung nicht erfüllt. Er entscheidet nicht nur ‚rational irrational‘ (*Bounded Rationality*), indem er seine Entscheidungskosten (rational) minimiert.<sup>13</sup> Vielmehr begeht er klassisch-ökonomisch nicht erklärbare Denkfehler.<sup>14</sup> Dies drückt sich in Urteils- und Entscheidungsfehlern aus (hier insgesamt: Verhaltensanomalien).<sup>15</sup> Verhaltensanomalien treten insbesondere – aber nicht nur – dann auf, wenn der Mensch schnell und automatisch entscheidet.<sup>16</sup>

Urteilsfehler beziehen sich auf die Fähigkeit, Wahrscheinlichkeiten korrekt einzuschätzen und neue Informationen korrekt zu verarbeiten.<sup>17</sup> Der Mensch bedient sich hierbei sog *Heuristiken* und hat (als Folge) sog *Biases*.<sup>18</sup> Heuristiken, beschrieben zuerst von *Kahneman/Tversky*,<sup>19</sup> sind abgekürzte Entscheidungen.<sup>20</sup> Die bekannteste Heuristik ist wohl die *Availability Heuristic*, nach der Wahrscheinlichkeiten anhand (leicht) verfügbarer Informationen bewertet werden.<sup>21</sup>

Entscheidungsfehler treten auf, wenn Entscheidungen nach gewissen Kriterien systematisch ineffizient sind.<sup>22</sup> Biases sind hierfür ein zentraler Grund. Zu den bekanntesten und wirkmächtigsten Biases zählen etwa der *Default Bias*, der *Confirmation Bias* und der *Optimism Bias*.<sup>23</sup> Entscheidungsfehler treten auch dann auf, wenn der Mensch statt auf Nutzenmaximierung nur auf Gewinne und Verluste relativ zu seiner aktuellen Situation achtet. Dabei gewichtet er (relative) Gewinne und Verluste nicht gleich (*Prospect Theory*).<sup>24</sup> Zwei Effekte spielen hier insbesondere eine Rolle: der *Endowment Effect* (auch *Loss Aversion*) sowie das *Framing*.<sup>25</sup>

b) *Ausnutzung von Verhaltensanomalien*. Entscheidungen, die unter Verhaltensanomalien zustande kommen, sind nicht – wie man vermuten könnte – unvorhersehbar. Vielmehr sind Menschen in ihrer Irrationalität berechenbar („*Predictably Irrational*“<sup>26</sup>). Studien können belegen, welche Effekte gewisse Heuristiken und Biases auf die Entscheidungsfindung haben. Dark Patterns – bzw. ihre Verwender – nutzen dieses Wissen über die Urteils- und Entscheidungsfehler des Menschen aus.<sup>27</sup>

Frühe Studien belegen dieses Verhalten für Anbieter etwa von Kreditkarten, Mobiltelefonartefakten und Druckern. Diese passen ihre Produkte so an, dass sie damit Verhaltensanomalien der Kunden ausnutzen.<sup>28</sup> Vor allem Urteilsfehler, insbesondere der Optimism Bias, sind hiervon betroffen. Anbieter ziehen einen Vorteil daraus, dass Konsumenten die Eintrittswahrscheinlichkeit eines bestimmten Ereignisses falsch einschätzen. Wer etwa die eigene Solvenz überschätzt, greift zu günstigen Kreditkarten mit hohen Straf- und Zinszahlungen bei Zah-

lungsausfall.<sup>29</sup> Der Wettbewerb zwischen Anbietern macht die Ausnutzung insofern sogar zur ökonomischen Notwendigkeit, da sie auf diesem Weg Gewinne steigern können.<sup>30</sup>

Im Unterschied zu diesen früher untersuchten Phänomenen beziehen sich Dark Patterns nicht auf ein Produkt selbst,<sup>31</sup> sondern nehmen die gesamte Entscheidungsumgebung in den Blick. Dies vervielfältigt die Möglichkeit, Verhaltens-

- 7 Vgl. zu diesem Erklärungsansatz *Bösch/Erb et al.*, Proceedings on Privacy Enhancing Technologies (PoPETs) 2016, 237 (244 ff.); s. auch *Schneider/Weinmann et al.*, Commun. ACM 2018, No. 7, 67 (69); *Mathur/Acar et al.*, Proc. ACM Hum.-Comput. Interact. CSCW 2019, Article 81, 6 und 13.
- 8 Einführend *Mathis/Steffen* in *Mathis*, European Perspectives on Behavioural Law and Economics, 2015, 31.
- 9 Vgl. *Korobkin/Ulen*, Cal. L. Rev. 2000, 1051 (1060 ff.); darstellend etwa *Chatziathanasiou/Leszczynska*, RW 2017, 314 (326 f.); *Steinbeck/Lachenmaier*, NJW 2014, 2086 (2087 f.).
- 10 Vgl. *Tversky/Kahneman*, The Journal of Business 1986, 251 (252 f.); *Hacker*, Verhaltensökonomik und Normativität, 2017, 36 ff.
- 11 Grundlegend *Coase*, Economica 1937, 386 (391 ff.); s. statt vieler *Cooter/Ulen*, Law & Economics, 6. Aufl. 2012, 88.
- 12 *Kirchgässner*, Homo Oeconomicus, 2008, 62 ff.; *Kirchgässner*, JZ 1991, 104 (106).
- 13 Grundlegend *Simon*, The Quarterly Journal of Economics 1955, 99 (sog Satisficing-Model). Vgl. auch *Stigler*, J. Pol. Econ. 1961, 213 (sog Optimal Decisionmaking Procedure-Model); s. hierzu *Eisenberg*, Stan. L. Rev. 1995, 211 (214 ff.); *March*, Bell J. Econ. 1978, 587 (590 ff.).
- 14 Einführend *Weber/Schäfer*, Der Staat 2017, 561 (568 ff.). A. A. *Gigerenzer/Gaissmaier*, Annual Rev. Psychology 2011, 451 (457 f.): „Ecological Rationality“.
- 15 Siehe *Jolls/Sunstein et al.*, Stan. L. Rev. 1998, 1471 (1477); *Hanson/Kysar*, N. Y. U. L. Rev. 1999, 632 (645 ff.); *Thaler* in *Medema/Samuels*, Foundations of Research in Economics: How do Economists do Economics?, 1996, 227 (230 ff.). Kritisch hierzu *Posner*, Stan. L. Rev. 1998, 1551.
- 16 Sog System 1-Denken („fast“), im Gegensatz zu System 2-Denken („slow“); sog Two-Systems oder Dual Process Theory. Vgl. *Kahneman*, Thinking, Fast and Slow, 2011.
- 17 *Hacker*, Verhaltensökonomik und Normativität, 80 ff.; s. auch *Hanson/Kysar*, N. Y. U. L. Rev. 1999, 632 (645).
- 18 Vgl. etwa *Baron* in *Zamir/Teichman*, The Oxford Handbook of Behavioral Economics and the Law, 2014, 3 (11).
- 19 *Kahneman/Tversky*, Cognitive Psychology 1972, 430 (430 ff.); s. auch *Tversky/Kahneman*, Science 1974, 1124.
- 20 Zu einem anderen Ansatz s. *Gigerenzer/Gaissmaier*, Annual Rev. Psychology 2011, 451 (454 ff.), die Heuristiken als uU besseren und adaptiven Entscheidungsweg sehen; s. auch *Gigerenzer/Todd* in *Gigerenzer/Todd/ABC Research Group*, Simple Heuristics That Make Us Smart, 2000, 3.
- 21 *Tversky/Kahneman*, Cognitive Psychology 1973, 207 (208 ff.). Für eine andere Klassifizierung *Gigerenzer/Gaissmaier*, Annual Rev. Psychology 2011, 451 (460 ff.).
- 22 *Pi/Parisi et al.* in *Zamir/Teichman*, The Oxford Handbook of Behavioral Economics and the Law, 2014, 143 (145); *Tversky/Kahneman*, Science 1974, 1124 (1124).
- 23 Vgl. etwa *Hanson/Kysar*, N. Y. U. L. Rev. 1999, 632 (645 ff.); vgl. auch *Hacker*, Verhaltensökonomik und Normativität, 80 ff.
- 24 Grundlegend *Kahneman/Tversky*, Econometrica 1979, 263 (274 ff.); s. statt vieler *Chatziathanasiou/Leszczynska*, RW 2017, 314 (327 f.). Zu weiteren Theorieansätzen vgl. *Schmolke*, Grenzen der Selbstbindung im Privatrecht, 2014, 198 ff.; *Hacker*, Verhaltensökonomik und Normativität, 63 ff.
- 25 *Hanson/Kysar*, N. Y. U. L. Rev. 1999, 632 (673 ff., 684 f.).
- 26 *Ariely*, Predictably Irrational, 2010.
- 27 Grds. bereits *Hanson/Kysar*, N. Y. U. L. Rev. 1999, 632 (724 ff.); *Bar-Gill*, Minn. L. Rev. 2008, 749 (765 ff.). Siehe auch *Wagner/Eidenmüller*, ZfPW 2019, 220 (230 f.).
- 28 *Bar-Gill*, Minn. L. Rev. 2008, 749 (761 ff.); *Bar-Gill*, U. Chi. L. Rev. 2006, 33 (38 ff.).
- 29 *Bar-Gill*, Minn. L. Rev. 2008, 749 (786); *Bar-Gill*, U. Chi. L. Rev. 2006, 33 (48 ff.).
- 30 *Hanson/Kysar*, N. Y. U. L. Rev. 1999, 632 (726 ff.). Wesentliche Gegenargumente, wie die Heterogenität zwischen Nutzern (*Epstein*, U. Chi. L. Rev. 2006, 111 [121]) und das „many bias problem“ (Interaktion verschiedener Anomalien, *Schwartz*, Stan. L. Rev. 2015, 1373 [1379, 1390 f.]) sind wohl bereits empirisch widerlegt (hierzu *Bar-Gill*, Minn. L. Rev. 2008, 749 [766 ff.]). Jedenfalls eröffnet die Möglichkeit, Dark Patterns zu personalisieren, einen wirksamen Weg, diese Probleme zu umgehen (sog Screening).
- 31 Etwa *Bar-Gill*, Minn. L. Rev. 2008, 749 (765 ff.); *Hacker*, Eur. R. Priv. L. 2017, 266 (269 ff.): „exploitative contracts“.

nomalien auszunutzen. Dabei können Anbieter alle Verhaltensanomalien des Nutzers gezielt ansprechen und insoweit exogene Ursachen für Fehlentscheidungen (iSe Präferenzverfehlung) hervorrufen.<sup>32</sup>

Die eingangs genannten Beispiele zur Gestaltung von Entscheidungsumgebungen im Internet machen dies deutlich: Voreinstellungen sprechen den Default Bias an; Countdowns zielen auf schnelles und automatisches Denken; Verweise auf Knappheit schaffen Loss Aversion; Verweise auf das Verhalten anderer Nutzer bedienen die Availability Heuristic und den Confirmation Bias; bestimmte Arten, Fragen und Informationen zu präsentieren, zielen auf Framing. Schließlich können farbliche und sonstige graphische Gestaltungen von Benutzeroberflächen sowie der Zwang zu entscheiden all diese Effekte verstärken und verschleiern.

Demnach ließen sich Dark Patterns ebenso als *Dark Nudging* einordnen, um den verhaltenspsychologischen Hintergrund herauszustellen.<sup>33</sup>

### 3. Verbreitung und Wirksamkeit von Dark Patterns in der Praxis

Aussagen darüber, wie verbreitet Dark Patterns in der Praxis sind, lassen sich bisher nur begrenzt treffen. Einerseits liegen nur wenige Studien vor. Andererseits bestehen definitorische Unklarheiten, da die bisher durchgeführten Studien keine streng verhaltenswissenschaftliche Definition anlegen. *Mathur et al.* stellen auf 11 % der untersuchten 11.000 Shopping-Webseiten die Verwendung von Dark Patterns fest.<sup>34</sup> *Utz et al.* hingegen kommen zu dem Ergebnis, dass ca. 57 % der untersuchten Cookie-Banner Dark Patterns nutzen.<sup>35</sup>

Auch die Bewertung der Wirksamkeit von Dark Patterns ist noch nicht abschließend möglich. Die vorhandenen Studien – aus der Perspektive des UI-Designs – zeigen gleichwohl beachtliche Steuerungseffekte. *Utz et al.* messen einen signifikanten Effekt unterschiedlicher Anzeigepositionen von Cookie-Bannern auf Bildschirmen.<sup>36</sup> *Luguri/Strahilevitz* stellen fest, dass „milde“ und „aggressive“ Dark Patterns im Vergleich mit der Kontrollgruppe um 14 bzw. 41 %-Punkte erhöhte Zustimmungswerte erreichen.<sup>37</sup> Zudem indiziert die allgemeine verhaltenswissenschaftliche Literatur an sich bereits starke Effekte von Verhaltensanomalien,<sup>38</sup> die sich wiederum durch gezieltes Ausnutzen aktivieren lassen.

In Summe ist die Annahme gerechtfertigt, dass Dark Patterns eine beträchtliche Verbreitung finden sowie eine große Wirkung haben können.

### 4. Besondere Gefahren in der Digitalen Welt

Dark Patterns sind dabei kein Phänomen, das alleine in der Online-Welt auftritt.<sup>39</sup> Doch erst in der digitalen Welt bildet sich ihre spezifische Gefährlichkeit und Prävalenz heraus.<sup>40</sup>

a) *Gezieltes Testen.* Anbieter können die Wirksamkeit von Design-Entscheidungen durch Labor- oder Feldtests gezielt untersuchen und steigern. Klassische A/B-Tests bieten ihnen die Möglichkeit, die Effekte verschiedener Gestaltungsvarianten auf das Entscheidungsverhalten zu untersuchen.<sup>41</sup> Dies ist im digitalen Kontext besonders bedeutsam.<sup>42</sup> Digitalkonzerne mit Millionen Nutzern haben fast unerschöpfliches Versuchsmaterial. Wie stark sie dieses Potenzial ausschöpfen ist noch wenig erforscht. Doch sind solche Experimente bekannt.<sup>43</sup> *Google* etwa hat einmal 40 „shades of blue“ auf ihre Interaktionsraten getestet.<sup>44</sup>

a) *Personalisierung.* Big Data, also das Sammeln und Auswerten riesiger Datenmengen, eröffnet zudem die Möglich-

keit, individuelle Nutzerprofile zu erstellen. Personalisierte Werbung wie auch etwa personalisierte Suchergebnisse sind bereits Gang und Gäbe.<sup>45</sup> Personalisierte, individuell diskriminierende Preise sind Realität.<sup>46</sup> Eine Aufklärung von Verbrauchern durch personalisierte Informationen ist ebenso denkbar wie personalisiertes Recht.<sup>47</sup>

Mit Hilfe derselben Methoden können Anbieter wohl auch *Personalized Dark Patterns* erstellen und anwenden.<sup>48</sup> Grundlage hierfür könnte etwa das *Comprehensive Assessment of Rational Thinking* (CART) sein – eine Methode, die ‚Rationalität‘ messbar macht.<sup>49</sup> Je nachdem, welche Verhaltensanomalie einen Nutzer besonders stark prägt, bekäme dieser ein anderes Benutzerinterface angezeigt. Dass dies erfolgsversprechend ist, legt eine erste Untersuchung nahe. Sie zeigt, dass bestimmte persönliche Umstände die Wirksamkeit eines Dark Pattern beeinflussen können.<sup>50</sup>

### II. Schutzpflicht gegenüber der Ausnutzung von Verhaltensanomalien

Angesichts dieser Bedrohungslage für die (innere) Autonomie jedes Einzelnen,<sup>51</sup> stellt sich die Frage, ob und wie das

32 Die von *Wiedemann/Wank*, JZ 2013, 340 (341 ff.), und ähnlich *Eidenmüller*, AcP 2010, 67 (82 ff.), vorgenommene Unterscheidung zwischen exogenen und endogenen Ursachen für „Abweichungen vom Rationalmodell“ bzw. „Präferenzstörungen“ geht hingegen implizit davon aus, dass gewisse (oder sogar alle) Verhaltensanomalien als solche dem Handelnden bzw. dem Dritten zuzurechnen sind. Dies vermag so nicht zu überzeugen.

33 *Richard Thaler* selbst spricht von „Sludge“, *Thaler*, Science 2018, 431; hierzu auch *Reisch*, Wirtschaftsdienst 2020, 87 (90).

34 *Mathur/Acar et al.*, Proc. ACM Hum.-Comput. Interact. CSCW 2019, Article 81, 1, die jd. nur textliche Elemente und einzelne, maschinell auswertbare Teilbereiche von Shopping-Webseiten (26 f.) untersuchen.

35 *Utz/Degeling et al.* in *Cavallaro/Kinder et al.*, ACM CCS '19 Proceedings, 2019, 973 (976). Nach *Nouwens/Licardi et al.*, ACM CHI '20 Proceedings, Paper 194, 5 nutzen 56,2 % teilweise Opt-out.

36 *Utz/Degeling et al.*, ACM CCS '19 Proceedings, 973 (980 f.).

37 *Luguri/Strahilevitz*, Shining a Light on Dark Patterns, University of Chicago Public Law Working Paper No. 719, 2019, 20 ff.

38 Zu Digital Nudging vgl. *Schneider/Weinmann et al.*, Commun. ACM 2018, No. 7, 67. Kritisch *Schwartz*, Stan. L. Rev. 2015, 1373 (1390 ff.).

39 *Hanson/Kysar*, N. Y. U. L. Rev. 1999, 632 (727 ff.) haben die offline-Gefahren schon früh erkannt.

40 So ließe sich auch von „Dark Digital Nudging“ sprechen.

41 *Schneider/Weinmann et al.*, Commun. ACM 2018, No. 7, 67 (72). Dies lässt, mit Blick auf die praktische Wirksamkeit von Dark Patterns, das „Wissensproblem“ (*Hacker*, Verhaltensökonomik und Normativität, 143) in den Hintergrund rücken.

42 *Rieger/Sinders*, Dark Patterns: Design mit gesellschaftlichen Nebenwirkungen, 10 f.

43 *Kohavi/Deng et al.* in *Grossman/Uthurusamy et al.*, ACM KDD '13 Proceedings, 2013, 1168; vgl. auch die Dokumentation bei <https://goo.dui.org/>.

44 *Hern*, Why Google has 200 m reasons to put engineers over designers, 2.5.2014, abrufbar im Internet: <https://www.theguardian.com/technology/2014/feb/05/why-google-engineers-designers> (Stand: 24.3.2020).

45 Vgl. etwa *Zuiderveen Borgesius*, IEEE Secur. Privacy 2013, 82; *Art.-29-Datenschutzgruppe*, Stellungnahme 2/2010 zur Werbung auf Basis von Behavioural Targeting, 22.6.2010.

46 *Tillmann/Vogt*, VuR 2018, 447 (447 ff.).

47 *Sunstein*, U. Pa. L. Rev. 2013, 1 (48 ff.); *Porat/Strahilevitz*, Mich. L. Rev. 2014, 1417 (1422 ff.); *Busch*, U. Chi. L. Rev. 2019, 309 (313 ff.); *Hacker*, Eur. R. Priv. L. 2017, 266.

48 In diese Richtung *Hacker*, Eur. R. Priv. L. 2017, 266 (270); aus UI-Perspektive *Conti/Sobieski*, IEEE Secur. Privacy Mag. 2009, 72 (73). *Schwartz*, Stan. L. Rev. 2015, 1373 (1380) übersieht dies.

49 *Stanovich/West et al.*, The Rationality Quotient, 2016.

50 *Luguri/Strahilevitz*, Shining a Light on Dark Patterns, 27 ff.

51 Vgl., wobei die *sedes materiae* iRd Grundrechte str. ist, *Lüdemann*, Edukatorisches Staatshandeln, 2004, 110 ff.: „Einstellungsfreiheit“; *Kolbe*, Freiheitsschutz vor staatlicher Gesundheitssteuerung, 2017, 215 ff.: Schutz individueller Wertvorstellungen; *Kreßner*, Gesteuerte Gesundheit, 2019, 207 ff.: Schutz der freien Willensbildung (forum internum); früh bereits *Faber*, Innere Geistesfreiheit und suggestive Beeinflussung, 1968, 58 ff.: „innere Geistesfreiheit“.

Recht hierauf reagieren muss. Insofern wendet sich die Perspektive des Verfassungsrechts gegenüber verhaltenswissenschaftlichen Erkenntnissen von der abwehrenden zur schützenden. Das Bekanntwerden des Nudging<sup>52</sup> als Regulierungsinstrument und das Konzept des „liberalen Paternalismus“<sup>53</sup> verlangten die Neubewertung und Fortentwicklung der Grenzen staatlicher Verhaltenssteuerung. Angesichts des Phänomens der Dark Patterns stellen sich diese Herausforderungen nun für den verfassungsrechtlichen Schutzauftrag des Rechts.

### 1. Herleitung der Schutzpflicht

Sowohl eine verfassungsrechtliche Analyse wie auch ein ökonomischer Blick erhellen, dass das Recht nicht nur rechtspolitisch aufgerufen, sondern grundrechtlich gezwungen ist, Dark Patterns wirksam zu begrenzen.

a) *Schutzpflicht zur Autonomiegewährleistung*. Sowohl im nationalen Verfassungs- als auch im Unionsrecht besteht eine auf Autonomiegewährleistung gerichtete Schutzpflicht.

Deutlich ausformuliert hat den Autonomieschutz das *BVerfG*. Seine Rechtsprechung zur (Privat-)Autonomie zeigt, dass das Verfassungsrecht zum Schutz vor der Ausnutzung von Verhaltensanomalien zwingt.<sup>54</sup> Nach den Entscheidungen zur Vertragsfreiheit (Art. 2 I GG)<sup>55</sup> muss der Staat die Voraussetzungen einer autonomen Entscheidung im Geschäftsverkehr sichern.<sup>56</sup> So setzt die Privatautonomie nach der *Handelsvertreter*-Entscheidung voraus, dass „die Bedingungen freier Selbstbestimmung tatsächlich gegeben sind“.<sup>57</sup> Pflichten zum Schutz der Privatautonomie greifen insbesondere in Fällen, in denen Selbst- in Fremdbestimmung umschlägt.<sup>58</sup> Dies gilt gerade mit Blick auf Situationen, in denen der Einzelne Entscheidungen über seine Daten trifft, also das informationelle Selbstbestimmungsrecht berührt ist.<sup>59</sup> Eben diese Schutzpflicht aktualisiert sich angesichts der Ausnutzung von Verhaltensanomalien. Denn auch diese Art der Verhaltenssteuerung rüttelt an der Autonomie des Nutzers. Die „Bedingungen freier Selbstbestimmung“ sind hier – aus verhaltenswissenschaftlicher Sicht – gerade nicht gegeben.

Eine solche Schutzpflicht gegen die Ausnutzung von Verhaltensanomalien fügt sich bruchfrei in den weitergehenden Gedanken des *BVerfG* zum Schutz der Autonomie als solcher (Art. 2 I iVm Art. 1 I GG).<sup>60</sup> In der Entscheidung zur *Sterbehilfe* betonte das Gericht jüngst, dass der Staat verpflichtet ist, Autonomie zu schützen.<sup>61</sup> Er hat „konkret drohenden Gefahren für die persönliche Autonomie vonseiten Dritter entgegenzuwirken“.<sup>62</sup> Der Staat kann und muss „[z]um Schutz der Selbstbestimmung“<sup>63</sup> tätig werden. Dementsprechend legt das *BVerfG* dem Staat die Pflicht auf, „dafür Sorge zu tragen, dass [Entscheidungen] tatsächlich auf einem freien Willen“ beruhen. Er hat insofern „Gefahren für die freie Willensbildung und die Willensfreiheit als Voraussetzungen autonomer Selbstbestimmung“ zu begegnen.<sup>64</sup>

Im Unionsrecht ist die Rechtslage weniger klar ausbuchstabiert. Doch ergeben sich aus dem datenschutzrechtlichen Recht auf Einwilligung des Art. 8 II 1 GRCh Pflichten zum Einwilligungsschutz.<sup>65</sup> Die Union hat den Auftrag, die „materielle Verantwortung des Betroffenen für seine Erklärung“<sup>66</sup> zu fördern. Eine derartige Schutzpflicht klingt auch im Schlussantrag des Generalanwalts zum *Orange România*-Fall an, wenn dieser ein „hohes Maß an Autonomie“<sup>67</sup> fordert.<sup>68</sup> Außerhalb des Bereichs der Datenverarbeitung lassen sich der Vertragsfreiheit iRd unternehmerischen Freiheit (Art. 16 GRCh)<sup>69</sup> sowie dem gebotenen hohen Verbraucher-

schutz (Art. 38 GRCh; Art. 169 I AEUV)<sup>70</sup> Pflichten zum Autonomieschutz entnehmen.<sup>71</sup>

b) *Schutzpflicht bei „Behavioral Market Failure“*. Eine Schutzpflicht gegenüber Dark Patterns lässt sich auch aus der Perspektive der ökonomischen Analyse des Rechts beschreiben.

aa) *Klassische Fälle des Marktversagens und „Behavioral Market Failure“*. Klassischerweise geht die Ökonomie davon aus, dass regulierende Eingriffe des Staates in den Markt nötig und gerechtfertigt sind, wenn ein Marktversagen vorliegt.<sup>72</sup> Ein Marktversagen erkennt die neo-klassische Theorie in drei Fällen an: bei externen Effekten, Marktmacht und Informationsasymmetrien.<sup>73</sup>

Verhaltensanomalien stellen sich nun als vierter Fall des Marktversagens dar (behavioralistisches Marktversagen bzw. „Behavioral Market Failure“).<sup>74</sup> Gemessen an den Effekten zeigen Verhaltensanomalien eine entscheidende Ei-

52 *Thaler/Sunstein*, Nudge, 2009; *Gerg*, Nudging, 2019.

53 Siehe Fn. 119.

54 Grds. *Isensee* in *Isensee/Kirchhof*, Hdb. d. Staatsrechts, Band IX, 3. Aufl. 2011, § 191 Rn. 97 ff. Dies andeutend etwa *Ohly*, „Volenti non fit iniuria“, 2002, 87 ff.

55 Grds. *Di Fabio* in *Maunz/Dürig*, GG, 89. EL, Art. 2 I Rn. 101 ff.; zum Problem der genauen Verortung im GG s. *Isensee* in *Isensee/Kirchhof*, Hdb. d. Staatsrechts, Band VII, 3. Aufl. 2009, § 150 Rn. 57 ff.

56 Siehe *Isensee* in *Isensee/Kirchhof*, Hdb. d. Staatsrechts, § 150 Rn. 97 ff. (der diese Entscheidungen jd. der unechten [sozialstaatlichen] Schutzpflicht zuordnet Rn. 100 ff.); Entscheidungsüberblick bei *Schmolke*, Grenzen der Selbstbindung im Privatrecht, 43 ff.

57 *BVerfGE* 81, 242 (255) = NJW 1990, 1469 (1470) = NZA 1990, 389.

58 *BVerfGE* 81, 242 (255) = NJW 1990, 1469 (1470) = NZA 1990, 389; auch *BVerfGE* 114, 73 (90) = NJW 2005, 2376 (2378). *Isensee* in *Isensee/Kirchhof*, Hdb. d. Staatsrechts, § 191 Rn. 98, 100.

59 *BVerfGK* 9, 353 = MMR 2007, 93 (93 f.) = r + s 2007, 29; *BVerfG*, NJW 2013, 3086 (3087 Rn. 20) = JZ 2013, 1156 (1157 Rn. 20) mit Anm. *Armbrüster*; kritisch *Klement*, JZ 2017, 161 (168 f.).

60 Vgl. etwa auch *BVerfGE* 60, 123 (133) = StAZ 82, 170 = NJW 1982, 2061 (2061); *BVerfG*, NJW 1999, 3399 (4001).

61 *BVerfG*, NJW 2020, 905 (909) Rn. 231 ff.

62 *BVerfG*, NJW 2020, 905 (910) Rn. 233.

63 *BVerfG*, NJW 2020, 905 (908) Rn. 217 und (920 f.) Rn. 338 f.

64 *BVerfG*, NJW 2020, 905 (910) Rn. 232 und (194) Rn. 275.

65 *Klement* in *Simitis/Hornung/Spiecker Döbmann*, DSGVO mit BDSG, 2019, Art. 7 Rn. 21 mwN; *Marsch*, Das europäische Datenschutzgrundrecht, 2018, 247 ff. Siehe auch *Franck/Purnhagen* in *Mathis, Law and Economics in Europe*, 2014, 329 (353 ff.). Grds. zu Art. 8 GRCh *Bernsdorff* in *Meyer/Hölscheidt*, Charta der Grundrechte der EU, 5. Aufl. 2019, Art. 8 Rn. 23.

66 *Klement* in *Simitis/Hornung/Spiecker Döbmann*, DSGVO mit BDSG, Art. 7 Rn. 23.

67 *GA Szpunar*, ECLI:EU:C:2020:158, BeckRS 2020, 2690 Rn. 44 – Orange România.

68 Vgl. insoweit auch *Bygrave/Tosoni* in *Kuner/Bygrave/Docksey*, GDPR, 2019, Art. 4 Nr. 11, C.1. 182.

69 Grds. *EuGH*, ECLI:EU:C:2013:521 = EuZW 2013, 747 = NZA 2013, 835 = BeckEuRS 2011, 622169 Rn. 32 – Alemo-Herron; *Kühling* in *Pechstein/Nowak/Häde*, FK zu EUV, GRCh und AEUV, 2017, Art. 16 GRCh Rn. 9.

70 Zur Einordnung als Rechtspflicht *Mörsdorf*, JZ 2010, 759 (760, 762); *Knops* in *Groeben/Schwarze/Hatje*, Europäisches Unionsrecht, 7. Aufl. 2015, Art. 38 GRCh Rn. 36 f.

71 Grds. *Sauerbaum*, EuR 2003, 390 (392 ff.).

72 *Schmolke*, Grenzen der Selbstbindung im Privatrecht, 124 ff.; *Grundmann*, JZ 2000, 1133 (1136 f.).

73 *Pindyck/Rubinfeld*, Mikroökonomie, 9. Aufl. 2018, 792; *Fritsch*, Marktversagen und Wirtschaftspolitik, 10. Aufl. 2018, 76; *Cooter/Ulen*, Law & Economics, 38 ff. Oft zusätzlich genannte öffentliche Güter sind als externe Effekte zu verstehen, vgl. *Fritsch*, Marktversagen und Wirtschaftspolitik, 80 ff.

74 *Hanson/Kysar*, N.Y.U.L. Rev. 1999, 632 (724 ff.); *Calo*, Geo. Wash. L. Rev. 2014, 995 (1000 ff.); bereits früh andeutend *Sunstein*, U. Chi. L. Rev. 1986, 1129 (1173) sowie *Eisenberg*, Stan. L. Rev. 1995, 211 (247), der jedoch zur „rational ignorance“ nicht klar abgrenzt; *Zamir*, Va.L. Rev. 1998, 229 (253 f.); *Bar-Gill*, Minn. L. Rev. 2008, 749 (765 ff.). AA *Lunn*, Journal of Consumer Policy 2015, 315 (321 ff.); *Fritsch*, Marktversagen und Wirtschaftspolitik, 324.

genschaft des Marktversagens: Sie führen dazu, dass Menschen Entscheidungen treffen, die mit ihren tatsächlichen Präferenzen nicht übereinstimmen.<sup>75</sup> Dies wiederum führt zu ineffizienten Allokationen, da den Betroffenen aus der Entscheidung nachteilige Folgen erwachsen,<sup>76</sup> also Abweichungen von pareto-optimalen Verteilungen entstehen.<sup>77</sup>

Ein Eingreifen bei der Ausnutzung von Verhaltensanomalien ist insofern gerade deshalb angezeigt, da sich Verhaltensanomalien weder durch Lerneffekte<sup>78</sup> noch durch Wettbewerb (als sog. *Market for Lemons*)<sup>79</sup> von selbst am Markt eliminieren.<sup>80</sup> Perspektivisch gilt dies insbesondere dann, wenn *Personalized Dark Patterns* in Rede stehen.<sup>81</sup> Die Heterogenität der Nutzer verkehrt sich in diesem Fall von einem potenziell wirkungsbeeinträchtigenden Faktor in einen wirkungsverstärkenden.<sup>82</sup>

bb) *Marktversagen als Schutzpflichtaktivierung*. Ökonomisch gesprochen erfüllt das Recht im Kontext wirtschaftlichen Handelns die Funktion, Marktineffizienzen zu vermeiden, mithin pareto-optimale Verteilungen sicherzustellen.<sup>83</sup> Folgt man diesem Ansatz, ist der ökonomische Imperativ, Marktversagen zu verhindern, aus grundrechtlicher Perspektive als Schutzpflichtaktivierung zu verstehen.

Ein solches ökonomisches Verständnis des Rechts fügt sich in die gegenwärtige Schutzpflichtdogmatik nahtlos ein. Denn das *BVerfG* erkennt bereits heute den Fall der Marktmacht als Auslöser einer Schutzpflicht an.<sup>84</sup> So statuiert das Gericht in der *Bürgerschaft*-Entscheidung bei einer „strukturelle[n] Unterlegenheit“ in einer „typisierbare[n] Fallgestaltung“<sup>85</sup> eine Schutzpflicht.<sup>86</sup>

Eine solche ökonomische Betrachtung findet auch im Unionsrecht eine tragfähige Grundlage. Die dortigen Schutzpflichten beziehen sich auf Fälle des Marktversagens, insbesondere auf Informationsasymmetrien und Marktmacht.<sup>87</sup> So erkennt der *EuGH* den Schutzzweck des Verbraucherschutzes darin, dass der Verbraucher sich „in einer schwächeren Verhandlungsposition befindet und einen geringeren Informationsstand besitzt“.<sup>88</sup>

Stellt die Ausnutzung von Verhaltensanomalien ein Marktversagen dar, greift das ökonomische Rational der *Bürgerschaft*-Entscheidung bzw. der unionsrechtlichen Schutzpflichten auch hier. In allen Fällen steht eine exogen induzierte Präferenzverfehlung, mithin Marktversagen, in Rede. Wo Marktversagen bzw. dessen Ausnutzung in „Fremdbestimmung“ mündet, muss der Staat sich schützend vor den Einzelnen stellen.<sup>89</sup>

c) *Ergebnis*. Beide Argumentationsansätze – der klassische Autonomieschutz sowie die ökonomische Analyse der Schutzpflichten – zeigen, dass eine Pflicht zum Schutz vor der Ausnutzung von Verhaltensanomalien besteht.<sup>90</sup>

Der Staat wird auf eine derart verstandene Schutzpflicht hin bereits heute „unterbewusst“ punktuell tätig. Dies zeigt sich daran, dass manche bestehenden Vorschriften als Schutz vor ineffizienten Konsequenzen von Rationalitätsdefiziten wirken. Ein Beispiel ist das Widerrufsrecht, das die Verbraucherrechte-RL für außerhalb von Geschäftsräumen geschlossene Verträge etabliert. Es bietet Schutz vor schnellem, automatischem Denken.<sup>91</sup>

Damit ist noch nicht gesagt, in welchem Umfang der Gesetzgeber und die anderen Staatsgewalten<sup>92</sup> mit Blick auf die Schutzpflicht als Untermaßverbot tätig werden müssen. Diese Grenze ist gerade wegen des gesetzgeberischen Einschätzungsspielraums schwer zu ziehen.<sup>93</sup> Dass angesichts der

gegenwärtigen Bedrohungslage ein Handlungsbedarf besteht, ist jedoch kaum zweifelhaft.<sup>94</sup>

## 2. Grenze zwischen Überzeugung und Manipulation

Das größte Problem im Umgang mit der Ausnutzung von Verhaltensanomalien stellt die Grenzziehung zwischen zunehmender Überzeugungsarbeit sowie verwerflicher Ausnutzung (Manipulation<sup>95</sup>) dar.<sup>96</sup>

a) *Ökonomische Definition einer Grenze*. Grundlage der ökonomischen Grenzziehung ist die Annahme, dass sich der Einzelne selbst Präferenzen setzt, die über die Zeit veränderbar, aber (ex ante) feststellbar sind.<sup>97</sup>

Eine grundsätzlich legitime Überzeugung findet statt, wenn der Einzelne seine Präferenzen aufgrund eines Angebots oder bereitgestellter Informationen anpasst. Diese theoretische Grenze ist praktisch gleichwohl schwer ermittelbar. Denn hierfür müssten Anzeichen bestehen, dass der Einzelne seine Präferenz geändert hat. Da jedenfalls Letzteres in spontanen Einwilligungssituationen nicht anzunehmen ist, besteht hierfür ein großer Begründungsaufwand.

Eine Manipulation liegt vor, wenn der Einzelne von seiner Präferenz abweicht, ohne diese zu ändern und ohne Vorliegen eines anderen als des behavioralistischen Marktver-

75 Siehe unten II. 2. a).

76 *Schwartz*, Stan. L.Rev. 2015, 1373 (1377 f., 1386 ff.): „mismatch cost“.

77 Vgl. *Schäfer/Ott*, Lehrbuch der ökonomischen Analyse des Zivilrechts, 4. Aufl. 2005, 107, 394 f.

78 Vgl. *Schmolke*, Grenzen der Selbstbindung im Privatrecht, 207 f.; etwa für Framing: *Kahneman/Tversky*, American Psychologist 1984, 341 (343).

79 *Eisenberg*, Stan. L.Rev. 1995, 211 (244). Hierfür etwa (noch) unter klassischer RCT *Schwartz/Wilde*, U.Pa.L.Rev. 1979, 630 (678 ff.). Grds. *Akerlof*, The Quarterly Journal of Economics 1970, 488 (489 ff.).

80 Insges. *Bar-Gill*, Minn. L.Rev. 2008, 749 (745 ff.); AA etwa *Epstein*, U. Chi. L.Rev. 2006, 111 (118 ff.).

81 Siehe oben I. 4. b.

82 Eben dies hat etwa *Epstein*, U. Chi. L.Rev. 2006, 111 (121) noch nicht gesehen.

83 *Eidenmüller*, Effizienz als Rechtsprinzip, 4. Aufl. 2015, 63; *Cooter/Ulen*, Law & Economics, 7 f.; hierzu *Martini*, Der Markt als Instrument hoheitlicher Verteilungslenkung, 2008, 166.

84 Klar ökonomische Argumentation etwa in *BVerfGK* 9, 353 = MMR 2007, 93 (93 f.) = r + s 2007, 29.

85 *BVerfGE* 89, 214 (232) = NJW 1994, 36 (38) = NVwZ 1994, 781 Ls.

86 Etwas anders in *BVerfGE* 81, 242 (255) = NJW 1990, 1469 (1470) = NZA 1990, 389; „starkes Übergewicht“ eines der Vertragsteile. Vgl. *Schmolke*, Grenzen der Selbstbindung im Privatrecht, 78 f.

87 Vgl. etwa MüKoBGB/*Basedow*, 8. Aufl. 2019, vor § 305 Rn. 4 ff.

88 St. Rspr., zuletzt *EuGH*, C-511/17, ECLI:EU:C:2020:188 = BeckRS 2020, 3211 Rn. 23 – Lintner.

89 Andeutend *BVerfGE* 108, 370 (393 f.) = NVwZ 2004, 329 (331): Schutz vor „Unterversorgung“.

90 Aus einer auf Allokationseffizienz ausgerichteten Sicht (ohne Marktversagen zu adressieren) etwa *Hanson/Kysar*, Harv. L.Rev. 1999, 1420 (1553 ff.) sowie *Hanson/Kysar*, Roger Williams U.L.Rev. 2000, 259. Siehe auch *Bar-Gill*, Minn. L.Rev. 2008, 749 (750): „substantial welfare loss“.

91 Vgl. etwa *Eidenmüller*, AcP 2010, 67 (82 ff.), noch zur Haustürgeschäfte-RL. Weniger klar *Purnhagen* in *Mathis*, European Perspectives on Behavioural Law and Economics, 2015, 51 (61 ff.).

92 Vgl. *Schmolke*, Grenzen der Selbstbindung im Privatrecht, 82 f., der gleichwohl die gerade im Datenschutzrecht bedeutende Exekutive nicht aufgreift.

93 *BVerfGE* 77, 381 (405); *EuGH*, C-112/00, ECLI:EU:C:2003:333 = EuZW 2003, 592 Rn. 82 – Schmidberger.

94 So bereits *Sunstein*, U. Chi. L.Rev. 1986, 1129 (1173).

95 *Wood* in *Coons/Weber*, Manipulation, 2014: „Exploitation“.

96 Andeutend *Wiedemann/Wank*, JZ 2013, 340 (344). Siehe auch *Luguril/Strahilevitz*, Shining a Light on Dark Patterns, 43 ff. Als ungelöst beschreibend *Sunstein/Reisch*, EuCML 2019, 93 (95).

97 Sog. Self-Interest Version der Thick Conception of Rational Choice Theorie, vgl. *Korobkin/Ulen*, Cal. L.Rev. 2000, 1051 (1064 ff.); aA etwa *Stigler/Becker*, The American Economic Review 1977, 76 (76 ff.).

sagens. Dies ist tatsächlich nicht leicht feststellbar.<sup>98</sup> Entscheidender Indizcharakter kommt der potenziell steuernden Entscheidungsumgebung zu.

Eine besondere Schwierigkeit stellen intertemporale Präferenzen dar. Eine einfache Theorie der Urteils- und Entscheidungsfehler legt zugrunde, dass zu jedem Zeitpunkt nur eine Präferenz vorliegt. Dies ist oft jedoch nicht der Fall – wie etwa die häufig konkurrierenden Wünsche der Nutzer, einen Dienst in Anspruch zu nehmen und die eigenen Daten zu schützen, deutlich machen. In diesem Fall bestehen auseinanderfallende kurzfristige und langfristige Präferenzen, die im Ergebnis zum sog. *Privacy Paradox* führen.<sup>99</sup> In diesen Situationen bedarf es einer Konfliktregelung, um zu ermitteln, was die ‚eigentliche‘ Präferenz ist. Klassischerweise gibt die Ökonomie der langfristigen Präferenz den Vorrang (Idee der „multiple selves“<sup>100</sup>).<sup>101</sup> Nur so lassen sich Verhaltenssteuerungen sinnvoll einordnen. Das *BVerfG* sieht das wohl ebenso. In seiner *Sterbehilfe*-Entscheidung erkennt es das Problem und scheint langfristigen Präferenzen den Vorzug zu geben.<sup>102</sup> Der Maßstab für eine verwerfliche Manipulation ist also grundsätzlich die langfristige Präferenz.

Schließlich ist die Frage zu beantworten, wann im Fall einer Manipulation ein Eingreifen des Staates angezeigt ist. Ökonomisch gesprochen ist dies eine Kosten-Nutzen-Abwägung: Ein Eingreifen ist sinnvoll, wenn der Nutzen die Kosten überwiegt.<sup>103</sup> Nutzen sind die gesteigerte Präferenzreicherung, Kosten entstehen etwa aus dem Entscheidungsaufwand, der Rechtsanwendung und entfallenden Lerneffekten. Die Bestimmung im Einzelfall ist schwierig. Hier sind konkrete Maßstäbe noch zu entwickeln. Es liegt jedoch nahe, aus der Kosten-Nutzen-Bewertung einen risiko-basierten Ansatz abzuleiten. Der Nutzen einer Intervention ist umso höher, je stärker der Steuerungseffekt ausfällt bzw. je größer die Bedeutung des Entscheidungsergebnisses ist. Hier steigen zwar die Kosten etwa der Rechtsanwendung, jedoch nicht direkt-proportional (die Grenzkosten wachsen nicht gleichstark mit).

b) *Normative Grenze*. Die ökonomische Perspektive lässt sich jedoch nicht 1:1 als normativer Handlungsleitfaden heranziehen.<sup>104</sup> Das Recht verfolgt nicht bzw. nicht zwingend nur Effizienz als Ziel. Aus verfassungsrechtlicher Sicht ist es bedeutend, jede Schutzmaßnahme mit den Grundrechten der beteiligten Parteien – also des Anbieters wie des Nutzers – in diesem „mehrpolgigen Verfassungsverhältnis“<sup>105</sup> auszutarieren.

aa) *Seite des Anbieters: zu rechtfertigender Eingriff*. Der Anbieter kann sich auf die unternehmerische Freiheit (Art. 16 GRCh)<sup>106</sup> bzw. Berufsfreiheit (Art. 12 GG)<sup>107</sup> sowie die Meinungs- (Art. 5 I GG;<sup>108</sup> Art. 11 GRCh<sup>109</sup>) und allgemeine Vertragsfreiheit (Art. 2 I GG) berufen. So ist anerkannt, dass Wirtschaftswerbung hiernach geschützt ist.<sup>110</sup> Dies erfasst grundsätzlich jede absatzfördernde Kommunikation, auch in nicht-textlicher Form wie die generelle Aufbereitung und Darstellung eines Angebots.<sup>111</sup> Ist eine derartige Einflussnahme auf das Gegenüber grundrechtlich geschützt, sollte dies gleichermaßen für die Gestaltung von Entscheidungsarchitekturen,<sup>112</sup> mithin die Ausnutzung von Verhaltensanomalien anderer, gelten.<sup>113</sup>

Gleichzeitig sind Eingriffe in Form der Beschränkung von Verhaltenssteuerung nach dem Verhältnismäßigkeitsgrundsatz (Art. 52 GRCh) rechtfertigbar.<sup>114</sup> Dies zeigt bereits die Verfassungskonformität des Verbots unlauterer Wettbewerbspraktiken.<sup>115</sup>

bb) *Seite des Nutzers: Schutz und Eingriff*. Auf Seite des Nutzers stellt sich die grundrechtliche Lage schwieriger dar. Es eröffnet sich die verfassungsrechtlich intrikate Frage, wo beim Schutz vor Dark Patterns die Grenzlinie zwischen Schutzpflicht und Eingriff in die Privatautonomie bzw. in das Grundrecht auf Einwilligung (Art. 8 II 1 GRCh) verläuft.<sup>116</sup>

Idealer stellt der Schutz der freien, autonomen Entscheidung vor *Ausnutzung* keinen Paternalismus<sup>117</sup> dar – insbes. keinen sog. „weichen“<sup>118</sup> bzw. „liberalen“<sup>119</sup>. Zwar zielt der Ausnutzungsschutz wie weicher Paternalismus auf freie, rationale Entscheidungen.<sup>120</sup> Da Ausnutzungsschutz jedoch fremde Einflüsse abwehrt, wirkt er nicht freiheitsbegrenzend, son-

98 Siehe *Schwartz*, Stan. L. Rev. 2015, 1373 (1378).

99 Vgl. *Solove*, The Myth of the Privacy Paradox, GW Legal Studies Research Paper No. 2020-10, 2020, 11 ff., iE jd. nicht zustimmend, 18 ff.

100 *Posner*, Stan. L. Rev. 1998, 1551 (1556 f.); s. auch *Ulen* in *Zamir/Teichman*, The Oxford Handbook of Behavioral Economics and the Law, 2014, 92 (116 f.).

101 Alternativ lässt sich auch auf den Schutz von Präferenzen zweiter Ordnung (sog. Meta-Präferenzen bzw. „second-order preferences“) abstellen, vgl. grds. *Frankfurt*, The Journal of Philosophy 1971, 5 (6 ff.); zum so gerechtfertigten Paternalismus *Sunstein*, U. Chi. L. Rev. 1986, 1129; *Schmolke*, Grenzen der Selbstbindung im Privatrecht, 243. Oder das Verhältnis von ex-post zu ex-ante Präferenzen, *Zamir*, Va. L. Rev. 1998, 229 (245 f.).

102 *BVerfG*, NJW 2020, 905 (910) Rn. 244: freier Wille nur bei Suizidentschluss von gewisser „Dauerhaftigkeit“, nicht wenn „kurzfristig gefasst“.

103 *Zamir*, Va. L. Rev. 1998, 229 (253); *Sunstein*, U. Chi. L. Rev. 1986, 1129 (1173); *Schmolke*, Grenzen der Selbstbindung im Privatrecht, 153 ff.

104 Grds. hierzu *Hacker*, Verhaltensökonomik und Normativität, 9 ff., 206 ff.

105 *Calliess*, JZ 2006, 321 (325 f.).

106 Vgl. *EuGH*, C-477/14, ECLI:EU:C:2016:324 = EuZW 2016, 582 = BeckRS 2016, 80848 Rn. 156 – Pillbox 38 Ltd.

107 Vgl. *BVerfGE* 85, 248 (256) = NJW 1992, 2341 (2341).

108 Vgl. *BVerfGE* 71, 162 (175) = NJW 1986, 1533 (1533 f.) = NVwZ 1986, 551 Ls.; *BVerfGE* 102, 347 (359) = NJW 2001, 591 (591).

109 *EuGH*, C-547/14, ECLI:EU:C:2016:325 = EuZW 2016, 582 Ls. = BeckRS 2016, 80849 Rn. 146 ff. – Philip Morris Brands ua, insbes. zur Werbefreiheit.

110 Vorgenannte Fn., sowie etwa *Faßbender*, GRUR 2006, 965 (965 ff.).

111 Vgl. die Benetton-Bildwerbung, *BVerfGE* 102, 347 (359) = NJW 2001, 591 (591).

112 Hierzu *Thaler/Sunstein*, Nudge, 3 ff.; *Thaler/Sunstein et al.* in *Shafir*, The Behavioral Foundations of Public Policy, 2013, 428 (428 ff.).

113 Anders ggf. nach einer engen Tatbestandstheorie, vgl. grds. *Isensee* in *Isensee/Kirchhof*, Hdb. d. Staatsrechts, § 150 Rn. 99.

114 Insofern geht es nicht um eine Abwägung, vgl. hierzu *Isensee* in *Isensee/Kirchhof*, Hdb. d. Staatsrechts, § 150 Rn. 121 ff.

115 Vgl. *BVerfGE* 32, 311 (317) = NJW 1972, 573 (573); *BVerfGE* 102, 347 (360 f.) = NJW 2001, 159 (591 f.). Siehe auch *EuGH*, C-71/02, ECLI:EU:C:2004:181 = EuZW 2004, 439 (441) Rn. 51 = NJW 2004, 3550 Ls. – Karner; und *EuGH*, C-421/07, ECLI:EU:C:2009:222 = EuZW 2009, 428 (430) = PharmR 2009, 277 Rn. 27 – Damgaard.

116 Zu dieser Abgrenzung vgl. etwa *Klement* in *Simitis/Hornung/Spiecker/Döhmman*, DSGVO mit BDSG, Art. 7 Rn. 21 ff., 32. Vgl. auch *Schmolke*, Grenzen der Selbstbindung im Privatrecht, 72 ff.

117 Zur Def. *Dworkin* in *Zalta*, The Stanford Encyclopedia of Philosophy, Spring 2020. Etwas andere Def. *Kirste*, JZ 2011, 805 (806). Für eine Modifizierung eintretend *Shiffrin*, Philosophy & Public Affairs 2000, 205 (213 f.).

118 *ISe* nach seinem Zweck der Herstellung freiwilliger, rationaler Entscheidungen definierten Paternalismus; s. etwa *Dworkin* in *Zalta*, The Stanford Encyclopedia of Philosophy; *Eidenmüller*, JZ 2011, 814 (815); anders *Sunstein*, Yale L. J. 2013, 1826 (1855 f.) („means paternalism“). Grds. *Feinberg*, The Moral Limits of the Criminal Law – Volume 3: Harm to Self, 1986, 12, der weichen Paternalismus nicht als Paternalismus *ieS* einordnet, so auch *Kirste*, JZ 2011, 805 (807 f.).

119 *ISe* nach seinem Mittel der zwanglosen bzw. Entscheidungsfreiheit bewahrenden definierten Paternalismus, s. grds. etwa *Thaler/Sunstein*, American Economic Review 2003, 175; *Eidenmüller*, JZ 2011, 814 (815); *Hacker*, Verhaltensökonomik und Normativität, 219 f.; anders *Sunstein*, Yale L. J. 2013, 1826 (1858 ff.) („soft paternalism“).

120 Vgl. Fn. 118.

dern allein freiheitsermöglichend bzw. -erhaltend.<sup>121</sup> Hierin liegt schließlich die Abgrenzung zum den eigentlichen Willen verhindernden bzw. verändernden harten Paternalismus.<sup>122</sup> Auf dem schmalen Grat zwischen Schutz *vor* eigener Freiheit (Paternalismus) und Schutz *zu* eigener Freiheit (Marktfehlerkorrektur) fällt Ausnutzungsschutz Letzterer zu.<sup>123</sup>

Verfassungsrechtlich stellen solche Schutzmaßnahmen (insbes. als Verbote) – wie wohl sie einer Schutzpflicht folgen – einen Eingriff (jedenfalls in Art. 2 I GG<sup>124</sup>) dar.<sup>125</sup> Denn Autonomieschutzmaßnahmen (auch gegenüber Dritten) verkürzen jedenfalls faktisch (mittelbar<sup>126</sup>), durch Eingriffe in Verträge bzw. die Vertragsfreiheit sogar final,<sup>127</sup> Handlungsmöglichkeiten. Dies gilt gerade wegen der nicht sicher vorhersehbaren, überschießenden Wirkung (*false positives*) und sonstiger möglicher Kosten auf Seite des Nutzers.<sup>128</sup> Diesen Spagat macht auch das *BVerfG* in der *Sterbehilfe*-Entscheidung.<sup>129</sup> Anders gewendet: Die sich in der Schutzpflicht vollziehende Materialisierung der positiven Seite der (Privat-)Autonomie (Freiheit *zu*) stellt zugleich einen Eingriff in die negative Seite der (Privat-)Autonomie (Freiheit *von*) dar.<sup>130</sup>

Um gerechtfertigt zu sein, müssen die autonomiesichernden Vorteile<sup>131</sup> der Intervention also in einem angemessenen Verhältnis zu möglichen Nachteilen stehen. Folge hiervon ist, dass auch der Verhältnismäßigkeitsmaßstab einen risikobasierten Ansatz bei der Bewertung zulässiger Regelungen nahelegt.<sup>132</sup>

c) *Maßstäbe des risiko-basierten Ansatzes.* Der risiko-basierte Ansatz sollte entscheidend auf zwei Elemente abstellen: den Grad der Steuerung sowie die drohende Schadensschwere.<sup>133</sup>

Der *Grad der Steuerung* lässt sich als Häufigkeit bzw. Wahrscheinlichkeit der Abweichung von einer (möglichst) neutralen Entscheidungssituation definieren. Als stark zu beurteilen wäre dann etwa eine Verhaltenssteuerung, die eine Grenze von 25 %-Punkten Abweichung von der (hypothetisch) unbeeinflussten Entscheidung überschreitet. Dies zu bestimmen, ist jedoch schwierig.<sup>134</sup> Die Effektstärke ließe sich einerseits empirisch, quantitativ feststellen – durch Studien<sup>135</sup> oder indem Anbieter zur Herausgabe von Daten verpflichtet werden<sup>136, 137</sup>. Andererseits könnte eine qualitative Effekt-ermittlung anhand einer verhaltensökonomischen Klassifizierung von Dark Patterns genügen, um einen Steuerungseffekt anzunehmen. Danach wäre grundsätzlich etwa bei der Unterbindung jeder als stark zu beurteilenden Verhaltenssteuerung ein hoher Nutzen anzunehmen.<sup>138</sup>

Die *drohende Schadensschwere* wiederum bemisst sich – normativ wie ökonomisch – nach der Wertigkeit und der Schwere der zu befürchtenden Rechtsgutsverletzung.<sup>139</sup> Normativ ist etwa bei der Verarbeitung sensibler Daten oder besonders umfassender Datenmengen ein höherer Autonomiegrad zu fordern. Dies deckt sich mit der grundsätzlichen Regelungsidee der DSGVO (vgl. Art. 9 II a DSGVO). Ökonomisch ist dies sinnvoll, da bei einem derart definierten Schaden grundsätzlich höhere Nachteile aus einer Präferenzfrustration erwachsen. In diesen Situationen wäre dann der zulässige Steuerungseffekt abzusenken, etwa auf bereits schwache Verhaltenssteuerungen bzw. etwa 10–15 %-Punkte Unterschied oder gar eine Regelung, die eher zu dem für den Nutzer vorteilhaften Entscheidungsergebnis tendiert.

### III. Kein umfassender Schutz vor Dark Patterns de lege lata

Dark Patterns verändern auch die einfach-rechtliche Perspektive auf verhaltensökonomische Erkenntnisse. Im Zentrum

der bisherigen juristischen Debatte stand die Frage, inwieweit das Wissen um Verhaltensanomalien bestehende Regelungsstrategien, allen voran das Informationsmodell, in neuem Licht erscheinen lässt.<sup>140</sup> Angesichts von Dark Patterns geht es nun jedoch darum, zu bewerten, ob das einfache Recht auf die systematische Ausnutzung von Verhaltensanomalien vorbereitet ist und die Autonomie wirksam schützt.<sup>141</sup>

### 1. Verbraucherleitbild im Wettbewerbs- und Verbraucherschutzrecht

Die Ausgangslage hierfür scheint wenig vielversprechend. Gerade das (unionsrechtlich geprägte) verbraucher-schützensde Recht ist von einem am rationalen Entscheider festhalten- den (Verbraucher-)Leitbild durchzogen.<sup>142</sup> Dies gilt primär für das (europäische) Wettbewerbsrecht. Dieses stellt auf das Leitbild des Durchschnittsverbrauchers („average consumer“) ab, der „angemessen gut unterrichtet und angemessen aufmerksam und kritisch“ ist.<sup>143</sup> Doch auch im Verbrau-

121 IE auch *Neuner*, JZ 2020, 269 (273). AA wohl *Schmolke*, Grenzen der Selbstbindung im Privatrecht, 72 ff.

122 Siehe hierzu *Eidenmüller*, JZ 2011, 814 (815); *Feinberg*, The Moral Limits of the Criminal Law – Volume 3: Harm to Self, 12; anders *Sunstein*, Yale L.J. 2013, 1826 (1855 f.) („ends paternalism“). Siehe *Eidenmüller*, Effizienz als Rechtsprinzip, 358 ff.

123 Vgl. zum Regulierungsrecht *Hellermann* in *Nettesheim/Diggelmann/Lege*, Der Schutzauftrag des Rechts, 2011, 366 (390) mwN.

124 Zum umfassenden Schutz des forum externum etwa *Kreßner*, Gesteuerte Gesundheit, 203 ff.

125 IE auch *Kirste*, JZ 2011, 805 (810); *Neuner*, JZ 2020, 269 (270), der zurecht auf den Schutz auch von „first-order desire“ (Frankfurt, The Journal of Philosophy 1971, 5 [7 ff.]) abstellt; *Schmolke*, Grenzen der Selbstbindung im Privatrecht, 76; wohl auch *Aaen* in *Anderheiden/Bürkli et al.*, Paternalismus und Recht, 2006, 109 (133 ff.).

126 Zum Str. hierzu *Starck* in *v. Mangoldt/Klein/Starck*, GG, 7. Aufl. 2018, Art. 2 Rn. 20.

127 *BVerfGE* 89, 48 (61) = NJW 1993, 2923 (2923).

128 Vgl. *Schmolke*, Grenzen der Selbstbindung im Privatrecht, 162 ff.

129 Vgl. *BVerfG*, NJW 2020, 905 (908) Rn. 214 ff.: „mittelbar-faktischen Auswirkungen“ des § 217 StGB als „Eingriff auch gegenüber den suizidwilligen Personen“.

130 Vgl. *Hacker*, Verhaltensökonomik und Normativität, 233 ff.; iE auch *Kirste*, JZ 2011, 805 (813); *Schmolke*, Grenzen der Selbstbindung im Privatrecht, 72 ff., 77.

131 Daneben ließen sich auch drittschützende Ziele anführen, vgl. *Schmolke*, Grenzen der Selbstbindung im Privatrecht, 32 ff., bzw. die „gesamtwohlfahrtsfördernde Wirkung“ *Purnhagen/Reisch*, ZEuP 2016, 629 (650).

132 Gleichzeitig wirkt sich dies – was die Grenzen des Beitrags sprengt – auf die zu wählenden Schutzinstrumente aus; so iE auch *Schmolke*, Grenzen der Selbstbindung im Privatrecht, 77; *Aaen* in *Anderheiden/Bürkli et al.*, Paternalismus und Recht, 109.

133 Ähnlich zu Art. 24 DSGVO *Martini* in *Paal/Pauly*, DS-GVO BDSG, 2. Aufl. 2018, Art. 24 Rn. 28 ff. In diese Richtung auch *Hacker*, Verhaltensökonomik und Normativität, 668 ff.

134 Vgl. *Schwartz*, Stan. L. Rev. 2015, 1373 (1403).

135 Vgl. *EuGH*, C-210/96, ECLI:EU:C:1998:369 = EuZW 1998, 526 (528) = NJW 1998, 3183 (3184 f.) Rn. 31, 37 – Gut Springheide.

136 Siehe unten IV.1. sowie *Martini/Weinzierl*, RW 2019, 287 (306). Vgl. *Schwartz*, Stan. L. Rev. 2015, 1373 (1402 f.).

137 AA *Schwartz*, Stan. L. Rev. 2015, 1373, 1380 (1390 ff.), der hier unüberwindbare Probleme sieht.

138 Vgl. *Martini/Weinzierl*, RW 2019, 287 (303).

139 Alleine hierauf abstellend *Krönke*, Der Staat 2016, 319 (340).

140 Paradigmatisch *Ben-Shabar/Schneider*, U.Pa.L.Rev. 2011, 647 (705 ff.); *Hacker*, Verhaltensökonomik und Normativität, 429 ff.

141 Früh hierzu, jd. verhaltenswissenschaftlich noch wenig geschärft, *Wiedemann/Wank* JZ 2013, 340 (342 ff.).

142 Zur Geschichte dieses Leitbilds etwa *Mak*, Eur. R. Priv. L. 2011, 25 (28 ff.); *Achilles*, Vom Homo Oeconomicus zum Differenzierten Verbraucher, 2020, 91 ff.; *Weber*, ZRP 2020, 98 (98 ff.).

143 Auf Grundlage von *EuGH*-Rechtsprechung, vgl. *EuGH*, C-476/14, ECLI:EU:C:2016:527 = NJW 2016, 2557 (2557) = EuZW 2016, 790 = GRUR 2016, 945 = GRUR Int 2016, 937 = NZV 2016, 467 Rn. 30 – Citroën Commerce; auch *EuGH*, C-210/96, ECLI:EU:C:1998:369 = EuZW 1998, 526 (528) = NJW 1998, 3183 (3184 f.) Rn. 31, 37 – Gut Springheide. Nunmehr ausdrücklich in ErwGrd. 18 S. 2 UGP-RL sowie § 3 IV 1 UWG. Vgl. zur Orientierung am europäischen Recht *Köhler* in *Köhler/Bornkamm/Feddersen*, Unlauterer Wettbewerb, 38. Aufl. 2020, § 1 UWG Rn. 30.

cherschutzrecht<sup>144</sup> findet sich ein in das Informationsmodell eingebettetes und durch Rationalitätserwartung geprägtes Leitbild eines „aufzuklärenden Verbrauchers“ – gerade in der Rechtsprechung des EuGH.<sup>145</sup>

Damit soll nicht gesagt sein, dass hier ein reines *homo oeconomicus*-Bild vorherrscht. Der durchschnittliche bzw. der aufzuklärende Verbraucher hat – wenngleich in verschiedener Intensität – rechtlich anerkannte Informationsdefizite sowie eingeschränkte Informationsverarbeitungskapazitäten.<sup>146</sup> Doch rücken derartige Eingrenzungen nicht von der generellen – normativen – Rationalitätserwartung ab.<sup>147</sup> Entsprechend limitiert sind – *de lege lata* – die Möglichkeiten, den Einzelnen vor Dark Patterns zu schützen.<sup>148</sup>

## 2. Beispiel: Datenschutzrecht

Paradigmatisch zeigt sich der mangelnde Schutz vor Dark Patterns mithilfe eines verhaltensökonomischen Blicks auf das Datenschutzrecht – dem Musterbeispiel für „Selbstbestimmung als Legitimationsmodell“.<sup>149</sup> Dabei kommt dem Datenschutzrecht insofern eine zentrale Bedeutung zu, als Einwilligungen in Datenverarbeitungen eine zentrale Stelle in der digitalen Welt einnehmen. Dark Patterns haben hier potenziell weitreichende Konsequenzen.

a) *Keine wirksamen Grenzen durch Einwilligungsvoraussetzungen.* Die DSGVO definiert eine wirksame Einwilligung in Art. 4 Nr. 11. Für die Wirksamkeit sind drei Elemente zentral: Freiwilligkeit, Informiertheit und Unmissverständlichkeit.<sup>150</sup>

aa) *Freiwilligkeit.* Aufsichtsbehörden und Literatur definieren das Kriterium der Freiwilligkeit zumeist negativ. Freiwilligkeit wird vorausgesetzt und liegt nur in bestimmten Konstellationen nicht vor. Neben Fällen physischen Zwangs mangelt es hieran insbes. in sog *Take-it-or-leave-it*-Konstellationen (Art. 7 IV DSGVO).<sup>151</sup> Die hierzu ergangene Leitlinie des Europäischen Datenschutzausschusses (EDSA)<sup>152</sup> stützt dies. Hiernach fehlt die Freiwilligkeit neben Situationen der „Konditionalität“ auch in Fällen, in denen ein „Ungleichgewicht der Macht“ besteht.<sup>153</sup>

Nach dieser Begrenzung der Freiwilligkeit sind Dark Patterns, die etwa auf das Verhalten anderer verweisen, Countdowns vorsehen oder Voreinstellungen treffen, nicht problematisch. Ihr Wirkmechanismus beruht – wie das Vorliegen von Verhaltensanomalien an sich – nicht auf einem Machtungleichgewicht. Selbst der Fall, in dem ein Anbieter etwa durch die Vorspiegelung von Benachrichtigungen zum schnellen Handeln verführt, ist hiernach nicht heikel. Denn der gefühlte Entscheidungsdruck bezieht sich nicht auf eine Entscheidung für eine gewisse Einwilligung (also einer *Take-it-or-leave-it*-Situation), sondern alleine auf das Treffen einer Entscheidung an sich.<sup>154</sup>

bb) *Informiertheit.* Auch die Voraussetzung der Informiertheit schafft keinen befriedigenden Schutz. Entscheidend ist nach der DSGVO, dass der Einzelne die nach Art. 13, 14 erforderlichen Informationen „in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache“ (Art. 12) erhält.<sup>155</sup> Ziel dieser Informationsgabe ist dabei, dem Betroffenen „zu ermöglichen, Entscheidungen in Kenntnis der Sachlage zu treffen, zu verstehen, in was [er einwilligt]“.<sup>156</sup> Nach dem EDSA gilt, dass ohne diese Informationen „die Kontrolle durch den Nutzer illusorisch“<sup>157</sup> ist.

Diese Hürde vermag es nicht, Dark Patterns zu verhindern. Einerseits wirken diese grundsätzlich nicht auf der Ebene der

nach Art. 13, 14 DSGVO erforderlichen Informationen. Weitergehende Angaben und Hinweise, etwa auf das Verhalten anderer Nutzer oder einen Entscheidungscountdown, erfasst die Vorschrift nicht. Dark Patterns ziehen ihre Wirksamkeit jedoch gerade aus dem weiteren Rahmen der Entscheidung.

Selbst wenn es um ein Framing der nach Art. 13, 14 DSGVO erforderlichen Informationen geht, macht dies Informationen nicht unverständlich und stellt insoweit keinen Verstoß gegen die Anforderungen an das „Wie“ der erforderlichen Informationsgabe dar.<sup>158</sup> Diese zielen darauf, „Informationsermüdung vorzubeugen“ und zu verhindern, dass der Einzelne „bei der Suche nach einzelnen Themen umfangreiche Texte durchkämmen“ muss.<sup>159</sup> Informationen mit einem Framing sind verständlich, der Mensch verarbeitet sie nur nicht rational. Sie führen gerade nicht zu Ermüdung oder einem großen Verständnisaufwand. Entscheidend für einen Steuerungseffekt durch Framing sind vielmehr Verhaltensanomalien.<sup>160</sup>

cc) *Unmissverständlichkeit.* Wohl am hilfreichsten könnte das Erfordernis der Unmissverständlichkeit „in Form einer [...] eindeutigen bestätigenden Handlung“ (Art. 4 Nr. 11 DSGVO) sein. Der EDSA knüpft hieran einen bunten Strauß an Erfordernissen und Verböten, etwa die Voraussetzung einer „bewussten Handlung“, ohne „Zweifel an der Zustimmung

144 IsD Sonderprivatrechts für Verbraucher, insbes. der Klausel-RL, Preisangaben-RL, Verbraucherrechte-RL id Fassung d. RL 2161/2019/EU.

145 Dieser stellt sogar ausdrücklich auf den Durchschnittsverbraucher ab, vgl. *EuGH*, C-26/13, ECLI:EU:C:2014:282 = NJW 2014, 2335 (2338) = EuZW 2014, 506 Rn. 74 – Käsler. Siehe hierzu *Achilles*, Vom Homo Oeconomicus zum Differenzierten Verbraucher, 70 ff., 100 ff., 135 ff. *Grundmann*, FS W.-H. Roth, 2015, 181 (192 f.); *Tamm*, Verbraucherschutzrecht, 2011, 150 ff.; *Blaurock*, JZ 1999, 801 (802); *Weber*, VuR 2020, 9 (13 f.) zur Übertragung durch den *EuGH*.

146 *Franck/Purnhagen* in *Mathis*, Law and Economics in Europe, 329 (343 f.).

147 *Sibony*, Eur. R. Priv. L. 2014, 901 (902 ff.).

148 Insoweit hilft auch das Konzept des „vulnerable consumer“ bzw. „besonders schutzbedürftigen Verbrauchers“ hier nicht ab (vgl. hierzu etwa *Kobte*, VuR 2012, 338 [338 ff.]). Denn die verhaltensökonomische Forschung stellt grds. nicht statusbezogenen Verhaltensanomalien nur bei einzelnen, besonders verletzlichen Personengruppen fest, sondern betrifft grds. alle Menschen. Verhaltensanomalien korrelieren insbes. auch nicht mit benachteiligten sozio-ökonomischen Lagen, die das Konzept des „vulnerable consumer“ grds. in den Blick nimmt.

149 *Lindner*, AöR 2015, 542 (546).

150 *Klement* in *Simitis/Hornung/Spiecker Döbmann*, DSGVO mit BDSG, Art. 7 Rn. 48 ff.

151 *Klement* in *Simitis/Hornung/Spiecker Döbmann*, DSGVO mit BDSG, Art. 7 Rn. 48, 56 ff. Siehe auch *Heckmann/Paschke* in *Ehmann/Selmayr*, DSGVO, 2. Aufl. 2018, Art. 7 Rn. 51 ff.

152 *Europäischer Datenschutzausschuss*, Endorsement 1/2018, 25.5.2018.

153 *Europäischer Datenschutzausschuss*, Guidelines 05/2020 on consent under Regulation 2016/679, 4.5.2020, 7 ff., Rn. 16 ff.; hier und im Folgenden dt. Übersetzung zitiert nach der soweit relevant inhaltsgleichen Vorversion: *Art.-29-Datenschutzgruppe*, Leitlinien in Bezug auf die Einwilligung gemäß Verordnung 2016/679, 10.4.2018; siehe auch *BVerfGK* 9, 353 = MMR 2007, 93 (93) = r + s 2007, 29; *BVerfG*, NJW 2013, 3086 (3087 Rn. 20) = JZ 2013, 1156 (1157 Rn. 20) mit Anm. *Armbrüster*.

154 So iE etwa *Heckmann/Paschke* in *Ehmann/Selmayr*, DSGVO, Art. 7 Rn. 55. Hier könnte alleine das Widerrufsrecht nach Art. 7 III 1 DSGVO teilweise Abhilfe schaffen; vgl. zu den verhaltensökonomischen Problemen *Eidenmüller*, AcP 2010, 67 (83).

155 *Art.-29-Datenschutzgruppe*, Leitlinien für Transparenz gemäß der Verordnung 2016/679, 11.4.2018.

156 *Europäischer Datenschutzausschuss*, Guidelines 05/2020 on consent under Regulation 2016/679, 4.5.2020, 14, Rn. 62.

157 *Ebd.*

158 Nur hierauf bezieht sich Art. 12 DSGVO; vgl. Art. 12 I 1 DSGVO.

159 *Art.-29-Datenschutzgruppe*, Leitlinien für Transparenz gemäß der Verordnung 2016/679, 7 f.

160 Selbst wenn man eine zielgruppenspezifische Informationsaufbereitung fordern wollte (*Art.-29-Datenschutzgruppe*, Leitlinien für Transparenz gemäß der Verordnung 2016/679, 8), änderte dies nichts. Denn Verhaltensanomalien treten grds. bei allen Menschen auf.

mungsabsicht“, bis hin zur Pflicht des Verantwortlichen, die „warnende Wirkung“ der Einwilligung – die mit der „Müdigkeit gegenüber dem Anklicken“ abnimmt – sicherzustellen.<sup>161</sup> Gleichwohl leitet der EDSA hieraus konkret keine klaren Voraussetzungen ab – vielmehr gibt er Verantwortlichen die Pflicht auf, „dieses Problem zu lösen“.<sup>162</sup> Bestenfalls offenbart dies ein konfuse Bild des Entscheidungsprozesses. Spezifisch untersagt ist danach etwa nur ein Einwilligen durch Scrollen. Umfassend kann dies Dark Patterns nicht verhindern.

b) *Verbraucherleitbild im Datenschutzrecht.* Diese – zugegeben – schemenhafte Darstellung zeigt eines deutlich: Die gegenwärtigen Bestimmungen zur Einwilligung (in ihrer Interpretation durch Literatur und Aufsichtsbehörden) bieten grundsätzlich keinen umfassenden Schutz vor einer Ausnutzung von Verhaltensanomalien, mithin vor Dark Patterns. Zwar mag das Datenschutzrecht in der Lage sein, gewisse Dark Patterns zu unterbinden.<sup>163</sup> Wesentlich ist aber, dass das Datenschutzrecht die Ausnutzung von Verhaltensanomalien nicht als solche zu verhindern vermag.

Hierfür gibt es eine tiefgehende Erklärung. Ein rechtsökonomischer Blick belegt, was im Wettbewerbs- und Verbraucherschutz anerkannt ist: Dem Datenschutzrecht liegt gegenwärtig ein Menschenbild zugrunde, in dem der Einzelne selbstbestimmt und rational nach seinen Interessen entscheidet – soweit er die hierfür notwendigen Informationen hat.<sup>164</sup>

Die jüngste Entscheidung zu Voreinstellungen im Planet49-Fall macht dies deutlich. Der *EuGH* stellt dabei heraus, dass klare und umfassende Informationen „den Nutzer in die Lage versetzen, die Konsequenzen einer [...] Einwilligung leicht zu bestimmen“.<sup>165</sup> Dahinter steht die Annahme, der Einzelne könnte auf Grundlage umfassender Informationen die Folgen seines Handelns abschätzen.<sup>166</sup> Damit überträgt der *EuGH* das Menschenbild des aufzuklärenden, gleichwohl rationalen *homo oeconomicus* auf das Datenschutzrecht.

### 3. Punktueller verhaltenswissenschaftlich informierter Schutz

Trotz dieser diagnostizierten generellen Ausrichtung auf den rationalen Entscheider existieren erste Anzeichen für verhaltensökonomisch informierte Regulierungen zum Schutz vor Ausnutzungen von Verhaltensanomalien.<sup>167</sup>

Ein Beispiel findet sich im unionalen Wettbewerbsrecht. Die Kommission geht davon aus, dass die neugefasste UGP-RL verhaltenswissenschaftliche Erkenntnisse einbezogen hat. Dort sollen sich nunmehr wirksame Instrumente gegen Framing finden.<sup>168</sup> Insofern macht die Kommission deutlich, dass es die Aufgabe der nationalen Behörden und Gerichte ist, den irreführenden Charakter einer Geschäftspraktik auch unter Zugrundelegung verhaltensökonomischer Erkenntnisse zu bestimmen.<sup>169</sup>

Ebenfalls gehen punktuellen Regelungen, die sich mit Voreinstellungen beschäftigen, auf verhaltensökonomische Erkenntnisse zurück. Ein entsprechendes Verbot zustimmender Voreinstellungen etabliert seit dem Jahr 2008 Art. 22 Verbraucherrechte-RL. Ebenso enthält nun die DSGVO – anders als die Datenschutzricht-RL – Bestimmungen, die datenschutzunfreundliche Voreinstellungen verbieten (Art. 25 II, ErwGrd. 32 - *Data Protection by Default*).<sup>170</sup> Diese Regelungen sind als (explizite) Antwort auf den Default Bias zu lesen.<sup>171</sup>

Gegen die vielfältigen Formen von Dark Patterns schaffen gerade die Bestimmungen im Datenschutz- und Verbraucherschutzrecht jedoch keine Abhilfe. Dies liegt vor allem daran, dass es in ihrer Auslegung durch den *EuGH* und die Generalanwälte – etwa im Planet49-Fall – wie durch die Datenschutzbehörden und die herrschende Literatur oft noch an einer verhaltenswissenschaftlichen Einordnung fehlt. Alleine das Wettbewerbsrecht scheint sich durch eine weitere Offenheit auszuzeichnen<sup>172</sup> – gleichwohl bleibt diese bisher praktisch weitgehend ungenutzt. Auch fehlt eine handhabbare verhaltensökonomische Auslegung der Vorschriften.

### IV. Notwendiger Behavioral Turn im Recht

Aus der Pflicht zum Autonomieschutz sowie den Schutzdefiziten, welche die Rationalitätserwartung des Rechts hervorruft, lässt sich eine umfassende Erkenntnis ableiten. Zwar kann der Gesetzgeber idealisierte Leitbilder wählen – verhaltenswissenschaftliche Erkenntnisse genießen keine unmittelbare Normativität.<sup>173</sup> Der Schutzpflicht-Gedanke schlägt gleichwohl eine Brücke zu der Frage, welche normative Bedeutung verhaltenswissenschaftlichen Erkenntnissen zukommt. Grundrechtliche Schutzpflichten zwingen den Staat dazu, tatsächliche Gefahren anzuerkennen und sich daran auszurichten.

Um der verhaltensökonomischen Bedrohungen Herr zu werden, sollte so auf die informatorische Wende seit den 1960er Jahren eine behavioralistische Wende, ein *Behavioral Turn*<sup>174</sup> folgen. Konkret sind hierfür zwei Schritte erforderlich.

161 *Europäischer Datenschutzausschuss*, Guidelines 05/2020 on consent under Regulation 2016/679, 4.5.2020, 18 Rn. 87.

162 *Ebd.*, Rn. 88.

163 Vgl. in diese Richtung *Wiedemann/Wank*, JZ 2013, 340. So iE auch *Wagner/Eidenmüller*, ZfPW 2019, 220 (233).

164 Der bereits angesprochene Schutz vor „Informationsermüdung“ (wohl angelehnt an „information overload“, *Roetzel*, Business Research 2019, 479 [481 ff.]) bestätigt diesen Befund paradigmatisch; vgl. *Straetmans*, EuCML 2016, 199 (207 f.) zur UGP-RL. Grund für eine Informationsermüdung sind alleine fehlende Ressourcen, also begrenzte Rationalität im Sinne von Transaktionskosten, nicht jedoch Verhaltensanomalien im Sinne von klassisch-ökonomisch nicht erklärbaren Denkfehlern bei der Verarbeitung aufgenommener Informationen; so etwa *Schmolke*, Grenzen der Selbstbindung im Privatrecht, 180 f. Zu einem verhaltensökonomischen Erklärungsansatz vgl. *Thaler/Sunstein*, Nudge, 35.

165 *EuGH*, C-673/17, ECLI:EU:C:2019:801 = NJW 2019, 3433 (3437) = DStRE 2019, 1472 = EuZW 2019, 916 = GRUR 2019, 1198 = NVwZ 2019, 1745 = ZD 2019, 556 Rn. 74 – Planet49. Siehe auch *EuGH*, C-543/09, ECLI:EU:C:2011:279 = EuZW 2011, 484 (487) = ZD 2011, 79 Rn. 58 – Deutsche Telekom.

166 Vgl. grds. auch *Helleringer/Sibony*, Colum. J.Eur. L. 2017, 607 (623 ff.).

167 *Europäische Kommission*, Legacy Document Consumer Policy 2010-2014, 2015, 7. Positiv *Helleringer/Sibony*, Colum. J.Eur. L. 2017, 607; kritisch *Straetmans*, EuCML 2016, 199 (207 f.). Weiteres Bsp.: ErwGr. 17 VO (EU) Nr. 1286/2014 (PRIIP); vgl. *Jager*, EuCML 2019, 238 (242).

168 *Europäische Kommission*, Commission Staff Working Document – Guidance on the Implementation/Application of Directive 2005/29/EC on Unfair Commercial Practices, 4.12.2009, 31.

169 *Ebd.*, 32.

170 *Martini/Weinzierl*, RW 2019, 287 (295 ff.).

171 Siehe *Testori Coggi*, Behavioural insights in the Commission, 13.6.2012, abrufbar im Internet: <https://www.politico.eu/article/behavioural-insights-in-the-commission/> (Stand: 29.5.2020); *Martini/Weinzierl* RW 2019, 287 (295); dies übersehend etwa *Klement* in *Simitis/Hornung/Spiecker Döhmman*, DSGVO mit BDSG, Art. 7 Rn. 36.

172 *Schebesta/Purnbagen*, Eur. L.Rev. 2016, 590; *Straetmans*, EuCML 2016, 199 (209); *Purnbagen*, EJRR 2017, 437, zu positiven Signalen in der *EuGH*-Rspr.

173 Grds. *Hacker*, Verhaltensökonomik und Normativität, 206 ff.

174 *Mathis/Steffen* in *Mathis*, European Perspectives on Behavioural Law and Economics, 31 (31); *Schwartz*, Stan. L.Rev. 2015, 1373: „Regulating for Rationality“.

## 1. Verhaltenswissenschaftlich informierte Auslegungen bestehender Normen

Aus dem verfassungsrechtlichen Schutzauftrag folgt die Pflicht, bestehende Normen verhaltenswissenschaftlich informiert auszulegen.<sup>175</sup> Hierzu ist es notwendig, dass die mit der Auslegung betrauten Instanzen selbst einen Behavioral Turn in ihrem Normverständnis vollziehen. So wie die neoklassische Ökonomie die Vorstellung vom rational entscheidenden Individuum in das Recht und die Rechtsauslegung eingepflanzt hat, müssen alle Beteiligten ihr regulatorisches Leitbild nun an neue Erkenntnisse anpassen.

Vorhandene Normen zeigen sich hierfür vielfach offen.<sup>176</sup> Naheliegender Ansatzpunkt ist etwa im Datenschutzrecht die Voraussetzung der „Freiwilligkeit“ der Einwilligung. Bei ihrer Auslegung lässt sich der Regelungsgedanke der Voreinstellungsverbote (Art. 25 II DSGVO) fruchtbar machen. Deren Telos, namentlich der Schutz vor der Ausnutzung von Verhaltensanomalien, ist verallgemeinerungsfähig.<sup>177</sup> Entsprechend sollte grundsätzlich etwa jede Verhaltenssteuerung, bei der nach dem risiko-basierten Ansatz ein hohes Risiko besteht, zur Unfreiwilligkeit der Einwilligung iSd Art. 4 Nr. 11 DSGVO führen.

Um derartige Auslegungen in der Breite zur Anwendung zu bringen, stehen den zuständigen Behörden gerade im Datenschutzrecht, aber auch im Wettbewerbsrecht, vielfältige Hilfsmittel zur Verfügung. Die Datenschutzbehörden könnten erste Standards entwickeln, die der EDSA dann in Leitlinien oder einen Beschluss gießen kann. Außerdem können sie von ihren Ermittlungsbefugnissen Gebrauch machen. So ließe sich bei Anbietern herausfinden, ob diese Datenverarbeitungen im Rahmen von A/B-Tests durchführen und auf der Grundlage personenbezogener Daten personalisierte Dark Patterns verwenden.<sup>178</sup> Hieraus ließen sich wiederum Rückschlüsse auf Lenkungsgrad und potenzielle Schadensschwere ziehen.

## 2. Spezifischer rechtlicher Schutz

Schließlich muss der Gesetzgeber selbst aktiv werden und spezifischen Schutz vor Dark Patterns etablieren.<sup>179</sup> Das Methodenspektrum ist dabei – wie das *BVerfG* in der *Sterbehilfe*-Entscheidung anmerkt<sup>180</sup> – denkbar weit. Entscheidend sind Antworten, die Verhaltensanomalien als eigenes Marktversagen mit entsprechenden Korrekturbedarfen verstehen.<sup>181</sup> Ziel sollte eine möglichst steuerungsfreie Entscheidung – im Sinne eines *Debiasing* – sein,<sup>182</sup> die gleichzeitig die Leitlinien des risikobasierten Ansatzes wahr.

Änderungen der Vorgaben zur Informationsbereitstellung – insbesondere verhaltenswissenschaftlich angepasste Informationen – können nur ein Weg sein.<sup>183</sup> Denkbar wäre es auch, bewusst auf eine Weiterentwicklung bzw. ein Umlernen vorhandener Heuristiken zu zielen. Geht man davon aus, dass der Mensch nie bzw. nicht stets voll rational entscheiden wird, ließen sich so langfristig Fehler minimieren bzw. etwaige Vorteile von Heuristiken nutzen.<sup>184</sup> Solche Ansätze allein vermögen Dark Patterns aber nicht zu verhindern. Verhaltensanomalien bleiben trotz dieser Methoden bestehen.

Gerade mit Blick auf das Element des Ausnutzens von Verhaltensanomalien, das Dark Patterns in Abgrenzung zum zufälligen Bestehen entsprechender Rationalitätsdefizite besonders macht, liegt ein Verbot nahe.<sup>185</sup> Dies schlägt eine US-amerikanische Gesetzgebungsinitiative (DETOUR-Act) vor, die Dark Patterns einen Riegel vorschieben will.<sup>186</sup> Angesichts der schwierigen Abgrenzungsfragen sowie der po-

tenziellen Kosten einer derart weitgehenden Maßnahme scheint hier jedoch Vorsicht geboten.<sup>187</sup> Allein bei besonderen Schadensschweren, etwa in sensiblen Bereichen wie bei Gesundheitsdaten, wird man einen gegen Null gehenden Steuerungseffekt fordern können. Hinsichtlich der DSGVO spricht dies dafür, die Bestimmungen zur Einwilligung bei sensiblen Daten anzupassen. Der Unionsgesetzgeber sollte jedenfalls in Art. 9 II a DSGVO die Voraussetzung „[ausdrücklich] und ohne steuernden Einfluss“ aufnehmen und so den durch die Auslegung der Freiwilligkeitsvoraussetzung des Art. 4 Nr. 11 DSGVO gewährten Schutz punktuell ergänzen.

Von besonderer Bedeutung für eine effektive Eingrenzung von Dark Patterns ist zudem die Durchsetzung schützender Bestimmungen. Neben einer individuellen Rechtsverfolgung sollten gerade auch kollektive (durch Verbands- oder Musterfeststellungsklagen) und hoheitliche (etwa durch Wettbewerbs- und Datenschutzbehörden) Wege offenstehen.<sup>188</sup>

## V. Zusammenfassung und Ausblick

Dark Patterns stellen eine Herausforderung für das Recht dar. Die bisherige rechtliche Diskussion zu Behavioral Law and Economics hat diese noch nicht hinreichend erkannt. Sie dreht sich einerseits um den Einsatz verhaltenswissenschaftlicher Methoden als Regulierungsinstrument, andererseits um die Auswirkungen verhaltenswissenschaftlicher Einsichten auf etablierte Regulierungskonzepte.

Dark Patterns eröffnen eine dritte Perspektive auf verhaltenswissenschaftliche Erkenntnisse im Recht. Aus verhaltenswissenschaftlicher Sicht sind Dark Patterns Designs, die Verhaltensanomalien ausnutzen und den Nutzer so zu einem für ihn nachteiligen Verhalten steuern. Untersuchungen legen nahe, dass Dark Patterns eine große Verbreitung finden. Gleichzeitig besitzen sie potenziell eine hohe Wirksamkeit. Besondere Gefahren ergeben sich aus der Möglichkeit, diese in digitalen Kontexten gezielt zu testen und perspektivisch sogar zu personalisieren.

175 Vgl. etwa Eisenberg, Stan. L. Rev. 1995, 211 (225 ff.). Grds. *Di Fabio* in *Maunz/Dürig*, GG, Art. 2 I Rn. 109 ff. zur Pflicht der Gerichte. In diese Richtung auch *Datenethikkommission der Bundesregierung*, Gutachten, 2019, 96.

176 Vgl. etwa Sibony, Eur. R. Priv. L. 2014, 901 (922 ff.).

177 Martini/Weinzierl, RW 2019, 287 (303).

178 Siehe zum möglichen Vorgehen Martini/Weinzierl, RW 2019, 287 (305).

179 Vgl. auch die Empfehlung der *Datenethikkommission der Bundesregierung*, Gutachten, 102. Auch der Weg der Selbstregulierung – etwa unter dem Dach des Art. 40 DSGVO – wäre möglich, vgl. *Grafenstein/Hölzel et al.*, Nudging: Regulierung durch big data und Verhaltenswissenschaften, 2018, 104 ff.

180 *BVerfG*, NJW 2020, 905 (921) Rn. 339.

181 Vgl. Hacker, Verhaltensökonomik und Normativität, 482 ff., 564 ff.

182 Grds. Jolls/Sunstein, The Journal of Legal Studies 2006, 199.

183 Hierzu etwa Bar-Gill, Minn. L. Rev. 2008, 749 (797 ff.); Hacker, Verhaltensökonomik und Normativität, 444 ff. Etwa *Helleringer/Sibony*, Colum. J. Eur. L. 2017, 607 (624 ff.); *Straetmans*, EuCML 2016, 199 (205 ff.).

184 Vgl. hierzu den Ansatz von *Gigerenzer/Gaissmaier*, Annual Rev. Psychology 2011, 451 (456 f.): Heuristiken als „Adaptive Toolbox“.

185 Zur Vorsicht mahnd etwa *Eidenmüller*, JZ 2005, 216 (223 f.).

186 Sec. 3 (a) Deceptive Experiences to Online Users Reduction Act (DETOUR Act), 1084, 116th Congress (9.4.2019).

187 Vgl. auch den Streit um eine haftungsrechtliche Lösung: für verschuldensunabhängige Haftung *Hanson/Kysar*, Harv. L. Rev. 1999, 1420 (1553 ff.); aA *Henderson/Rachlinski*, Roger Williams U. L. Rev. 2000, 213 (244 ff.); erwidern *Hanson/Kysar*, Roger Williams U. L. Rev. 2000, 259 (313 ff.); zum deutschen Recht *Hacker*, Verhaltensökonomik und Normativität, 654 ff.

188 Grds. *Augenhofer*, EuZW 2019, 5 (9); *Micklitz*, Brauchen Konsumenten und Unternehmen eine neue Architektur des Verbraucherrechts?, 2012, 87 ff., 113 ff.; hierzu *Gsell*, JZ 2012, 809 (816 f.); s. auch *Grundmann*, FS W.-H. Roth, 181 (195 f.).

Grundrechtliche Schutzpflichten rufen staatliche Stellen angesichts der autonomiegefährdenden Wirkung von Dark Patterns zum Handeln auf. Das Unions- wie das nationale Verfassungsrecht gebieten einen wirksamen Autonomieschutz. Die praktische und grundrechtliche Grenze zwischen hinzunehmender Überzeugungsarbeit sowie (verwerflicher) Manipulation ist schwer zu ziehen. Ein risikobasierter Ansatz, der die Wirkungsgrade von Dark Patterns sowie drohende Schäden berücksichtigt, bietet einen ersten guten Anhaltspunkt.

Gleichzeitig schützt das einfache Recht nicht effektiv vor Dark Patterns. Vielmehr legen sie die bestehenden Schutzlücken und die noch wenig entwickelte Dogmatik im Umgang mit der Ausnutzung von Verhaltensanomalien offen. Entscheidend ist dafür eine Grunderkenntnis: Das Recht hängt dem Bild des rationalen Entscheiders an. Gegenwärtig schützt es Rationalität nicht – es setzt sie voraus.

Aus alledem leitet sich eine umfassendere Forderung ab: Es bedarf eines Behavioral Turn des Rechts. Notwendig ist ein Umsteuern, um den Gefahren, die Dark Patterns heraufbeschwören, wirksam begegnen zu können. Dabei geht es

nicht um eine soziale Aufladung des Rechts, sondern – dem Marktversagensargument folgend – einer Adjustierung am (markt-)liberalen Ideal selbst.<sup>189</sup>

Die Antwort des Rechts kann sich nicht darauf beschränken, etwa nur die Informationsgabe bzw. das Informationsmodell anzupassen – so jedoch die klassische Reaktion. Vielmehr geht es darum, die Rationalitätserwartung selbst zu adressieren und spezifische Antworten auf die Ausnutzung von Verhaltensanomalien zu finden.

Behörden und Gerichte können bestehende Normen hierfür vielfach im Geiste des verfassungsrechtlichen Schutzauftrags nutzen. Flankierend sind spezifische rechtliche Regelungen notwendig, die Autonomie originär schützen. Soll der Wert bzw. das Institut der Einwilligung insbesondere als Legitimationsmodell erhalten bleiben, muss das Recht sich diesen Herausforderungen stellen. ■

<sup>189</sup> Zu dieser klassischen Konfliktlinie im Verbraucherschutzrecht etwa Vogel, Verbrauchervertragsrecht und allgemeines Vertragsrecht, 2006, 39 ff.; s. auch Gsell, JZ 2012, 809 (814 ff.).