Spindler, Gerald

Article

Behavioral Economics und Verbraucherschutz sowie Sicherheitsrecht in der IT-Welt

Wirtschaftsdienst

Suggested Citation: Spindler, Gerald (2020) : Behavioral Economics und Verbraucherschutz sowie Sicherheitsrecht in der IT-Welt, Wirtschaftsdienst, ISSN 1613-978X, Springer, Heidelberg, Vol. 100, Iss. 2, pp. 97-99, https://doi.org/10.1007/s10273-020-2576-8

DOI: 10.1007/s10273-020-2576-8

Ende des vorherigen Zeitgesprächsartikels

Gerald Spindler

Behavioral Economics und Verbraucherschutz sowie Sicherheitsrecht in der IT-Welt

Behavioral Economics (Verhaltensökonomie) hat sich als eigenständige wirtschaftswissenschaftliche Forschungsrichtung etabliert, die die neo-institutionellen bzw. -klassischen Modelle aufgrund der verhaltenswissenschaftlichen Bezüge erheblich relativiert (und ihre Verhaltensannahmen des homo oeconomicus bzw. rational handelnden Menschen infrage stellt). Gerade für den Verbraucherschutz trägt Behavioral Economics dadurch, dass irrationale Verhaltensweisen einbezogen werden, dazu bei, neue Herangehensweisen und Ansätze zu berücksichtigen, allen voran das „Nudging“[1]. Aus juristischer Perspektive bietet Behavioral Economics im Verbraucherschutzrecht Hilfestellung für die Entwicklung neuer Schutzmechanismen, die von dem hergebrachten reinen Informationsmodell, wie es im europäischen Verbraucherschutzrecht noch immer dominiert, und den Cooling-off-Zeiten zur „Wiederherstellung“ des rationalen Verhaltens abrücken und andere Instrumente in den Vordergrund stellen. So kann aufgezeigt werden, dass das klassische Widerrufsrecht, wie etwa in § 355 BGB, als ein Opt-out-Recht weniger genutzt wird als es bei einer umgekehrten Gestaltung, eines Opt-in in Form einer nochmals erforderlichen Bestätigung des geschlossenen Vertrags der Fall wäre.[2]

Allerdings muss aus juristischer Perspektive immer im Blick behalten werden, dass Behavioral Economics anders als neo-klassische bzw. -institutionelle Modelle kaum verallgemeinerbare normative Aussagen treffen, da sie oft

1 R. Thaler, C. Sunstein: Nudge: Wie man kluge Entscheidungen anstößt, Berlin 2011.

2 G. Wagner, H. Eidenmüller: In der Falle der Algorithmen? Abschöpfen von Konsumentenrente, Ausnutzen von Verhaltensanomalien und Manipulation von Präferenzen: Die Regulierung der dunklen Seite personalisierter Transaktionen, in: Zeitschrift für die gesamte Privatrechtswissenschaft ZfPW, 2019, S. 220, S. 233 f.

Prof. Dr. Gerald Spindler ist Inhaber des Lehrstuhls für Bürgerliches Recht, Handels- und Wirtschaftsrecht, Multimedia- und Telekommunikationsrecht am Institut für Wirtschaftsrecht der Georg-August-Universität Göttingen.

auf verhaltenswissenschaftlichen Experimenten beruhen. Rechtliche Lösungen können aber oftmals nur auf einer gewissen Abstraktionshöhe entwickelt werden und sind nur in der richterlichen Praxis im Rahmen von Generalklauseln für den jeweiligen Einzelfall spezifizierbar – was gleichzeitig der Rechtssicherheit natürlich abträglich ist.

Behavioral Economics und Digitalisierung – Chancen

Gerade die Digitalisierung und die mit ihr ermöglichte Personalisierung eröffnet aber für die mehr einzelfallbezogene Analyse und ein auf den jeweiligen Verbraucher fein abgestimmtes Nudging neue Chance. Im Bank- und Kapitalmarktrecht ist schon seit langem sowohl auf der Grundlage vertragsrechtlicher Pflichten als auch Regulierungen in § 64 Abs. 3 Wertpapierhandelsgesetz das „know-your-customer"-Prinzip geläufig, dass den Anlageberater dazu verpflichtet, sich genaue Kenntnisse über das Risikoprofil und die Präferenzen des Kunden zu verschaffen,[3] damit aber auch über etwaige „Rationalitätsstörungen". Damit ist letztlich aber der große Bereich der personalisierten und auf individuelle Bedürfnisse abgestimmten Informationen angesprochen.[4] Da aber durch die Digitalisierung Daten der Konsumenten laufend erhoben werden, nicht zuletzt um Profile und damit personalisierte Werbung zu erstellen, liegt es auf der Hand, dass diese nicht nur zu Werbezwecken genutzt werden sollten, sondern auch Händler veranlassen müss(t)en, dieses Wissen für personalisierte Informationen im Rahmen des Verbraucherschutzes zu nutzen.[5] Dies muss nicht nur Händler betreffen, sondern kann auch gegenüber Plattformanbietern bzw. elektronischen Marktplätzen greifen, die ebenso wie Händler Daten über die Marktplatzteilnehmer sammeln, um Dienste personalisiert anzubieten. Dann aber müssen Händler sowie Plattformanbieter ihr Wissen nutzen, um Verbraucher auch vor Gefahren bzw. irrationalen Handlungen zu schützen, die z. B. nicht ihren Präferenzen oder ihrer Risikolage entsprechen.

Grenzen einer Personalisierung von Verbraucherinformationen ergeben sich allerdings durch den Datenschutz. Denn jede Personalisierung erfordert ein vorhergehendes Profil bzw. die Sammlung der entsprechenden Daten. So gilt nach Art. 5 Abs. 1 c Datenschutz-Grundverordnung (DSGVO) das Gebot der Datensparsamkeit; auch ist es nicht ohne weiteres möglich, Profile ex ante anzulegen, ohne dass z. B. ein Vertrag anvisiert wird. Erst bei Vertragsdurchführung kommen nach Art. 6 Abs. 1 b DSGVO die entsprechenden Rechtfertigungen zum Tragen; zuvor bedarf es überwiegender Interessen des Datenverarbeitenden, die nicht immer per se gegeben sein werden, Art. 6 Abs. 1 f DSGVO. Einwilligungen stoßen zudem auf schwer überwindbare Grenzen im Rahmen von Art. 7 DSGVO, insbesondere Art. 7 Abs. 4 DSGVO.

Zudem ist fraglich, ob eine (nationale) gesetzlich vorgeschriebene Personalisierung mit den verschiedenen Richtlinien zum Verbraucherschutz vereinbar ist, zuletzt etwa der Verbraucherrechterichtlinie.[6] Hier dominiert nach wie vor das Modell der möglichst umfänglichen Information des Verbrauchers, ohne dass eine Differenzierung nach Personen bzw. deren persönlichen Präferenzen und Individualitäten möglich wäre. Der voll harmonisierende Charakter aller Richtlinien in diesem Bereich sperrt (leider) nationale Bestrebungen, eine personalisierte Verbraucherschutzinformation einzuführen, da die Mitgliedstaaten keine darüberhinausgehenden Informationen durch Händler verlangen dürfen oder die Pflichten nicht modifizieren können.

Das sollte indes niemanden daran hindern, über rechtspolitische Alternativen bzw. neue Ansätze nachzudenken: So kann etwa einhergehend mit den Vorschlägen der Datenethikkommisson 2019 über die Einführung eines Treuhänders für persönliche Daten nachgedacht werden.[7] Wesentlich bedeutsamer sind die Möglichkeiten, den der Einsatz künstlicher Intelligenz (KI) auf Verbraucherseite bieten könnte: Denn wenn KI in der Lage ist, das Verhalten und die Bedingungen verschiedener Händler einzuschätzen, gleichzeitig aber auch das Verhalten des Verbrauchers, der die KI einsetzt, analysieren und verbessern kann, wäre es möglich, den Verbraucher in hohem Maße personenspezifisch vor verfehlten Entscheidungen zu schützen. Der Staat könnte solche KI-Lösungen in Gestalt von Open-Source-Software zur Verfügung stellen bzw. fördern, vergleichbar einer „Stiftung KI-Warentest".

3 Dazu näher mit weiteren Nachweisen G. Spindler, in: K. Langenbucher, D. H. Bliesener, G. Spindler: Bankrecht, Kap. 33, Rn. 97 f.; Bundesgerichtshof: Urteil vom 22.3.2011 – XI ZR 33/10, ZIP 2011, 756 = Neue Juristische Wochenschrift, 2011, 1949 Rn. 21; Bundesgerichtshof: Urteil vom 6.7.1993 – XI ZR 12/93, BGHZ 123, 126 = WM 1993, 1455 – Bond.

4 Vgl. hierzu auch C. Busch: Implementing Personalized Law: Personalized Disclosures in Consumer Law and Data Privacy Law, in: The University of Chicago Law Review, 86. Jg. (2019), S. 309 ff.

5 Vgl. allgemein zur Wissenszurechnung bei Big Data G. Spindler, A. Seidel: Die zivilrechtlichen Konsequenzen von Big Data für Wissenszurechnung und Aufklärungspflichten, in: Neue Juristische Wochenschrift, 2018, S. 2153.

6 Richtlinie 2011/83/EU des Europäischen Parlaments und des Rates vom 25. Oktober 2011 über die Rechte der Verbraucher, zur Abänderung der Richtlinie 93/13/EWG des Rates und der Richtlinie 1999/44/EG des Europäischen Parlaments und des Rates sowie zur Aufhebung der Richtlinie 85/577/EWG des Rates und der Richtlinie 97/7/EG des Europäischen Parlaments und des Rates, Amtsblatt L 304, S. 64 ff. vom 22.11.2011.

7 Vgl. dazu Datenethikkommission der Bundesregierung: Gutachten, Berlin, Oktober 2019, S. 133 (135), https://www.bmi.bund.de/SharedDocs/downloads/DE/publikationen/themen/it-digitalpolitik/gutachten-datenethikkommission.pdf?__blob=publicationFile&v=6 (9.1.2020).

Behavioral Economics und IT-Sicherheitsrecht

Aber nicht nur im Kern-Verbraucherschutzrecht kann der Nudging-Gedanke wichtige neue Ansätze hervorbringen, sondern auch im IT-Sicherheitsrecht. Bekanntlich ist das IT-Sicherheitsrecht trotz etlicher Reformen in den letzten Jahren, insbesondere durch die Reform des Gesetzes über das Bundesamt für Sicherheit in der Informationstechnik (BSIG), nach wie vor lückenhaft.[8] Zwar verpflichten jetzt §§ 8a ff. BSIG die Betreiber kritischer Infrastrukturen dazu, Vorkehrungen zur Sicherstellung der IT-Sicherheit zu treffen; auch hat die EU im „Cybersecurity-Act“[9] erstmals einen europaweiten Rahmen für Sicherheitszertifikate für IT-Produkte geschaffen, die gerade dem Verbraucher ermöglichen sollen, das Sicherheitsniveau der Produkte einzuschätzen. Dies entspricht Ansätzen, wie sie von der Bundesregierung zur Einführung eines IT-Sicherheitsgütesiegels verfolgt werden.[10] Da gerade Verbraucher das schwächste Glied in der Kette darstellen, indem ihre Geräte durch Schwachstellen von Dritten ausgenutzt werden können, z. B. für Botnetze, stellt dies im Prinzip einen begrüßenswerten Ansatz dar. Denn die typische Informationsasymmetrie im Verbraucherbereich gilt natürlich (und erst recht) für Sicherheitsfragen, für die Verbraucher in aller Regel wenig sensibel sind, da Gefahrenpotenziale und Risiken falsch eingeschätzt werden. Um solche Asymmetrien zu überwinden, eignet sich Signalling, indem z. B. Gütesiegel verwendet werden, die von vertrauenswürdigen Experten ausgestellt wurden, die dem Verbraucher die Einhaltung bestimmter Sicherheitsvorgaben „signalisieren“ können, sodass der Verbraucher selbst das Gefahrenpotenzial eines Produktes einschätzen kann.

Allerdings rufen gerade die Erkenntnisse der verhaltenswissenschaftlichen Forschung bzw. die Behavioral Economics Zweifel an der Eignung von Gütesiegeln zur Verbesserung der Produktsicherheit hervor, zumindest sind bestimmte Rahmenbedingungen auf Informationsmärkten erforderlich, um die Wahrnehmung von Gütesiegeln zu sichern. Denn der Einfluss von Gütesiegeln auf die Kaufentscheidung von Verbrauchern hängt davon ab, ob das Gütesiegel als einzig relevantes Kriterium wahrgenommen wird und der Verbraucher sich überhaupt der Bedeutung des Gütesiegels bewusst ist. Aus dem Bereich der freiwilligen Gütesiegel, etwa im Umweltbereich („blauer Engel“) oder im Lebensmittelbereich (z. B. die deutschen Bio-Siegel), ist bekannt, dass eine Vielzahl von verschiedenen Siegeln die Wirkung dieses Signals erheblich verwässern können, zumal sich Zweifel an der Seriösität von bestimmten Labels auf den ganzen Markt übertragen können. Hier können Ansätze aus der Verhaltensökonomie wichtige Einsichten bieten, wann und unter welchen Umständen Verbraucher tatsächlich auf Labels und „Beipackzettel“ reagieren, sodass die gewünschten Verhaltenseffekte eintreten.[11]

Allerdings sollte man sich hüten, allein auf Gütesiegel zu setzen, denn mindestens genauso wichtig wie ein IT-Sicherheitsdesign ist die laufende Anpassung von IT-Produkten an sich ändernde digitale Umgebungen, die bekannten Patches bzw. Updates. Diese werden allerdings allenfalls mittelbar von einem Gütesiegel umfasst, etwa wenn die Siegel-Prüfung auch diese einbezieht. Dies kann aber nicht eine eigenständige Regulierung aus Produktsicherheitssicht ersetzen, die breitflächig im Sinne von Verkehrspflichten für Hersteller und Importeure etc. eine Pflicht zu laufenden Updates und Kontrollen der Produkte im Hinblick auf neue digitale Umgebungen einführt.[12] So könnte etwa an eine Pflicht zur „IT-Security by Design“ gedacht werden – vergleichbar der in der DSGVO eingeführten „Privacy by Design“ (etwa Datenschutz durch Technikgestaltung), Art. 25 DSGVO – die den Verbraucher vor Installation eines Produktes schrittweise durch nötige Sicherheitseinstellungen führt. Insgesamt bedarf es eines Regulierungmixes aus stärkeren öffentlich-rechtlich und zivilrechtlichen Anreizen, Pflichten und Sanktionen, die in einem allgemeinen IT-Produktsicherheitsgesetz zusammen mit einer Mischung aus verhaltensbasierter Haftung und Gefährdungshaftung strukturiert sein sollte.

8 Vgl. allgemein zur Reform über kritische Infrastrukturen in der Informationstechnologie: D.-D. Kipker, D. Scholz: Das IT-Sicherheitsgesetz 2.0, in: Multimedia und Recht, 2019, S. 431 (433); G. Spindler: Verträge über digitale Inhalte – Anwendungsbereich und Ansätze – Vorschlag der EU-Kommission zu einer Richtlinie über Verträge zur Bereitstellung digitaler Inhalte, in: Multimedia und Recht, 2016, S. 147 (152); G. Hornung: Neue Pflichten für Betreiber kritischer Infrastrukturen: Das IT-Sicherheitsgesetz des Bundes, in: Neue Juristische Wochenschrift, 2015, S. 3334 f.

9 Verordnung (EU) 2019/881 des Europäischen Parlaments und des Rates vom 17. April 2019 über die ENISA (Agentur der Europäischen Union für Cybersicherheit) und über die Zertifizierung der Cybersicherheit von Informations- und Kommunikationstechnik und zur Aufhebung der Verordnung (EU) Nr. 526/2013 (Rechtsakt zur Cybersicherheit), Amtsblatt L 151, S. 15 ff. vom 7.6.2019.

10 Bundesamt für Sicherheit in der Informationstechnik: Die Lage der IT-Sicherheit in Deutschland 2019, 17.10.2019.

11 Vgl. zur Beeinflussung des Kaufverhaltens durch Gütesiegel: Deutsche Gesellschaft für Online-Forschung (DGOF): Gütesiegel beeinflussen Kaufverhalten, Studie, 13.4.2018, https://www.dgof.de/studie-guetesiegel-beeinflussen-kaufverhalten (9.1.2020); insbesondere zu Datenschutz-Gütesigeln: N. Jentzsch: Was können Datenschutz-Gütesiegel leisten?, in: Wirtschaftsdienst, 92. Jg. (2012), H. 6, S. 413, S. 416, https://www.wirtschaftsdienst.eu/inhalt/jahr/2012/heft/6/beitrag/was-koennen-datenschutz-guetesiegel-leisten.html (30.1.2020).

12 Vgl. zu Pflichten des IT-Herstellers nach Inverkehrgabe G. Spindler: Verantwortlichkeiten von IT-Herstellern, Nutzern und Intermediären, Bundesamt für Sicherheit in der Information, 2007, Rn. 127 ff., https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Studien/ITSicherheitUndRecht/Gutachten_pdf.pdf?__blob=publicationFile&v=2 (9.1.2020).