TAB
BÜRO FÜR TECHNIKFOLGEN-ABSCHÄTZUNG
BEIM DEUTSCHEN BUNDESTAG

Dark Patterns – Mechanismen (be)trügerischen Internetdesigns

Themenkurzprofil Nr. 30 | Christoph Bogenstahl | November 2019

Dark Patterns ist ein Sammelbegriff für Internetmuster oder -designs, die darauf ausgelegt sind, Nutzende von Onlinediensten und sozialen Netzwerken dazu zu bringen, Tätigkeiten auszuführen, die ihren eigentlichen Interessen zuwiderlaufen und mit negativen Konsequenzen verbunden sein können.

Stets werden dabei bestimmte menschliche Verhaltens- oder Wahrnehmungsmuster ausgenutzt. Dark Patterns werden unter anderem im Rahmen von Neuromarketing eingesetzt und gehören im weiteren Sinne zu den psychologischen Ansätzen der technologiegestützten Verhaltensbeeinflussung. Während die Beeinflussung im Sinne einer von Kunden gewünschten (Kauf-)Aktivität bzw. Verhaltensänderung durch Überzeugung – wie etwa das Beenden gesundheitsgefährdender bzw. die Initiierung gesundheitsfördernder Aktivitäten (z.B. mithilfe von Gesundheits-Apps) – zumeist transparent erfolgt (und auch positiv konnotiert sein kann), werden Dark Patterns üblicherweise verschleiert. Vergleichbar ist dieser Ansatz in etwa mit Social Bots, die ebenfalls bewusst getarnt werden und vortäuschen, echte (menschliche) Nutzer zu sein, um eine Wahrnehmungs- und ggf. Verhaltensänderung herbeizuführen.

Mit Dark Patterns werden beispielsweise bestimmte Emotionen angesprochen, um zu einem Kauf im Internet zu verleiten oder einen bestimmten Link anzuklicken. Andere Muster sind darauf ausgelegt, gezielt die Aufmerksamkeit von wesentlichen Aspekten abzulenken, z.B. von einer erhöhten Rechnung oder versteckten Kosten. Preisvergleiche oder das Rückgängigmachen von Aktionen werden häufig erschwert. Ebenso gehören getarnte Werbung oder Produkte, die sich beim Onlinekauf „in den Warenkorb schleichen“ (Sneak into Basket), zu Dark Patterns. Es werden somit manipulativ Zusatzkäufe forciert oder auch verdeckt Kundendaten gesammelt.

Der Einsatz von Dark Patterns ist unethisch, mitunter unlauter und ggf. betrügerisch. Insbesondere sind auf die Ausnutzung menschlicher Wahrnehmungsschwächen ausgerichtete Dark Patterns für unerfahrene Nutzende schädlich, z.B. Senioren, Kinder und Jugendliche sowie bildungsferne Gruppen. Aus Sicht des Verbraucherschutzes werden Verbraucherinnen und Verbraucher über Dark Patterns gezielt gesteuert, manipuliert und getäuscht. Es bedarf einer besonderen Aufmerksamkeit der Nutzenden, diese Manipulationen und deren typischen Muster zu erkennen und zu umgehen. Eine regulatorische Herausforderung besteht darin, Dark Patterns aufzudecken, da diese in aller Regel verschleiert werden, um ihren Zweck zu erfüllen.

Hintergrund und Entwicklung

Der Begriff Dark Patterns umfasst mehrere Beispiele für Designmuster von Internetseiten, die darauf ausgelegt sind, Nutzende zu Handlungen zu verleiten, die deren eigentlicher Intention zuwiderlaufen. Mögliche Folgen können beispielsweise die ungewollte Preisgabe persönlicher Daten oder der Kauf unerwünschter Produkte, Dienstleistungen und Abonnements sein. Häufig werden mit Dark Patterns bestimmte menschliche Verhaltens- oder Wahrnehmungsmuster gezielt manipulativ ausgenutzt. Zu den Bereichen, in denen Dark Patterns zum potenziellen Nachteil von Nutzenden eingesetzt werden, zählen der Onlinehandel mit Waren und Dienstleistungen, weitere Onlinedienste wie E-Mail-Dienste, Downloadportale und Suchmaschinen sowie soziale Netzwerke, wie beispiels-

weise Twitter, Instagram, WhatsApp und Facebook. Einige der Dark Patterns sind hinsichtlich des zugrundeliegenden Mechanismus miteinander verwandt. Auch werden häufig mehrere Dark Patterns gemeinsam verwendet, um den gewünschten Effekt zu verstärken und die wahre Intention zu verschleiern. Bekannte Beispiele von Dark Patterns lassen sich in drei Untergruppen einteilen:

- Ködern, Täuschen und Ausüben emotionalen Drucks,
- Entlocken von Daten und
- Ablenken und Hervorrufen von Ermüdung.

Ködern, Täuschen und Ausüben emotionalen Drucks

Webseitendesigns können darauf ausgelegt werden, bestimmte Emotionen anzusprechen, um zu einem Kauf im Internet zu verleiten oder einen bestimmten Link anzuklicken (Bait and Switch). Die Nutzerin bzw. der Nutzer will eigentlich eine bestimmte Aktion ausführen, das Design verleitet aber dazu, stattdessen eine andere auszuführen, die eigentlich gar nicht intendiert war. Ein bekannt gewordenes Beispiel war Microsofts fehlgeleiteter Ansatz, Menschen dazu zu bringen, ihre Computer auf Windows 10 zu aktualisieren. Die Umstellung auf Windows 10 – als ein eigentlich gänzlich neues Programm – über das Windows Update Center wurde als „notwendiges Update" deklariert. Diese Täuschung löste Proteste aus und wurde als „Upgrade Gate" bezeichnet (Thurrott 2016).

Gelegentlich wird Werbung auch als Inhalt der Seite oder der Navigationsführung ausgegeben, um den Benutzer dazu zu bringen, auf diese zu klicken, obwohl dies gar nicht vorgesehen war. Gewohnte Verhaltensmuster bei der Navigation auf Webseiten werden dazu missbraucht, einen falschen Klick zu provozieren und auf eine Werbeseite zu gelangen. Diese zweifelhafte Praxis ist beispielsweise bei beliebten Softwaredownloadportalen gängige Praxis. Die Haupteinnahmequelle dieser Anbieter ist in der Regel Displaywerbung. Oft werden Anzeigen geschaltet, die wie ein Downloadbutton aussehen und die Benutzenden dazu bringen, auf die Anzeigen zu klicken, anstatt – wie eigentlich beabsichtigt – den Softwaredownload zu starten. Bei den zur 1&1-Gruppe gehörenden Mailanbietern GMX und web.de werden Werbebanner zwischen dem normalen Maileingang positioniert. Klickt man versehentlich auf die als Mail getarnte Werbung, können ungewollt kostenpflichtige Zusatzabonnements abgeschlossen werden (Verbraucherzentrale NRW e.V. 2017).

Eine eher unterschwellige Art der Manipulation ist das Provozieren von Verunsicherungen und Schuldgefühlen. Dabei wird die Möglichkeit zur Ablehnung eines Waren- oder Dienstleistungsangebots so formuliert, dass die Nutzenden in Verlegenheit geraten. Beispielsweise wird suggeriert, durch die Ablehnung des Angebots eine unkluge Entscheidung zu fällen. Die Ablehnung eines kostenlosen Probeabonnements wird etwa mit dem Text „Nein danke, ich will keine unbegrenzte Expresslieferung.", „Nein danke, ich bin reich genug." (Verzicht auf vermeintliche Sparmöglichkeiten) oder auch „Nein danke, ich gehe das Risiko ein." beim Verzicht auf ein Versicherungspaket unterlegt. So werden subtil Schuldgefühle erweckt, da mit der Einwilligung vermeintlich nur Vorteile verbunden sind und die Ablehnung einer Verschwendung oder dem Eingehen eines (großen) Risikos gleichkäme. Es werden allgemein sozial akzeptierte Normen und Werte adressiert, wie das Vermeiden von Verschwendung, das Sparen als Tugend oder die Risikovermeidung. Der so aufgebaute personalisierte soziale Druck soll die Wahrscheinlichkeit erhöhen, das Angebot doch anzunehmen – wider besseres Wissen und entgegen der ursprünglichen Intention. Ähnlich funktionieren Dark Patterns, die darauf ausgerichtet sind, Stress zu erzeugen, indem ein Gefühl von Dringlichkeit erzeugt wird: Es werden Angebote präsentiert, die man angeblich „gerade knapp verpasst hat". Der Eindruck wird durch die visuelle Art der Präsentation verstärkt (Proschofsky 2019). Diese Dark Patterns sind in der Reise- und Tourismusbranche verbreitet.

Entlocken von Daten

Trickfragen zielen darauf ab, der Nutzerin bzw. dem Nutzer Antworten zu entlocken, die eigentlich gar nicht herausgegeben werden wollten – beispielsweise während des Ausfüllens eines Internetformulars. Der Trick basiert darauf, dass die Webseite beim Lesen nur flüchtig erfasst wird und dabei entscheidende Details nicht oder nur unzureichend wahrgenommen werden. Bei sorgfältigem Lesen würde es vermutlich zu einer anderen Einschätzung und Entscheidung kommen. Dies ist z.B. dann der Fall, wenn mehrere Optionen über eine Reihe von Kontrollkästchen gegeben werden, wobei die Bedeutung der Kontrollkästchen wechselt. Bedeutet das Aktivieren der Checkbox in einem Fall noch „Opt-out" („Bitte senden Sie mir keine Informationen zu."), wechselt die Bedeutung zu „Opt-in" in einem anderen

Fall („Bitte senden Sie mir Informationen zu."). Will der Nutzende keine Werbung erhalten, müsste die erste Checkbox aktiviert werden und nicht die zweite. Die Wirkung wird häufig durch verwirrende Formulierungen verstärkt.

Als unethisches Design können auch irreführende Privatsphäreeinstellungen (Privacy Zuckering) gesehen werden, die darauf ausgelegt sind, Nutzenden mehr persönliche Informationen zu entlocken, als diese eigentlich zu geben beabsichtigen. Bei Nutzung einer bestimmten Dienstleistung geben Kunden beispielsweise ungewollt die Erlaubnis, ihre personenbezogenen Daten an Dritte zu verkaufen. Datenbroker kaufen so entstehende Datensätze und kombinieren sie mit anderen online hinterlassenen Datenspuren zu einem Profil, das sie dann wiederum weiterverkaufen. Derlei Profile können Informationen über private Vorlieben oder die körperliche und geistige Gesundheit enthalten. Für Konsumenten ist es mitunter sehr schwierig, sich gegen die Vermittlung der Daten zu entscheiden, da die Nutzung und Verkettung der Daten über Drittanbieter verschleiert sind und im Kleingedruckten verschwinden.

Bei dem verwandten Freundespam (Friend Spam) werden E-Mail- oder Social-Media-Berechtigungen unter dem Vorwand erschlichen, dass diese für ein gewünschtes Ergebnis zwingend notwendig wären, wie beispielsweise „Freunde finden". Später wird jedoch die Berechtigung missbraucht, um Spam an alle Kontakte zu versenden. Ein bekannt gewordenes Beispiel für dieses Dark Pattern wurde von LinkedIn verwendet. Als Teil des Anmeldeprozesses wurde empfohlen, Zugang zu dem E-Mail-Konto zu gewähren. Im Gegenzug wurde versprochen, dass es „Ihrer Karriere ein starkes Netzwerk" bietet. In einem nächsten Schritt wurde die unverfänglich klingende Schaltfläche „Zum Netzwerk hinzufügen" angeboten. Tatsächlich wurde hiermit LinkedIn die Erlaubnis erteilt, jeden Kontakt automatisiert mit einer Einladung zu LinkedIn zu kontaktieren. Dieser Schritt war für viele der neuen LinkedIn-Kunden überraschend und nicht intendiert. In einer Sammelklage wurde diese Praxis nach kalifornischem Recht als illegal befunden. LinkedIn wurde im Ergebnis im Jahr 2015 mit einer Geldstrafe von 13 Mio. US-Dollar belegt.

Ablenken und Hervorrufen von Ermüdung

In anderen Fällen schleichen sich beim Onlinekauf Produkte in den Warenkorb (Sneak into Basket). Es wird darauf spekuliert, dass Kundinnen und Kunden unaufmerksam sind und dies nicht bemerken. Dies ist beispielsweise dann der Fall, wenn sich der Einkauf einer Ware oder Dienstleistung über mehrere aufzurufende bzw. zu blätternde Seiten erstreckt und sich ein zusätzlicher Artikel oder Mehrwertdienst (Zusatzversicherungen o.Ä.) erst zu einem späteren Zeitpunkt unerwartet im Warenkorb befindet. Dies kann geschehen, falls eine aktivierte Checkbox auf einer vorherigen Seite übersehen wurde. Dieses Designmuster ist aus der Werbewirtschaft auch als Trägheitsverkauf (Inertia Selling) bekannt. Hier werden Produkte an Verbraucherinnen und Verbraucher unverlangt zugesendet und diese dann zugleich dazu aufgefordert, dafür zu zahlen. Ein ähnliches Dark Pattern – die erzwungene Fortführung – liegt beispielsweise dann vor, wenn die kostenlose Testversion eines Services endet und von den Kunden ungewollt in eine Bezahlvariante überführt wird. In einigen Fällen wird dies noch verschärft, indem es seitens des Anbieters bewusst erschwert wird, die Mitgliedschaft zu kündigen.

Ähnlich funktionieren Designs, die Nutzende in eine Situation locken sollen, aus der ein Ausweg sehr kompliziert ist. So kann eine bestimmte Leistung beispielsweise schnell und mit wenigen Mausklicks online bestellt werden, während für das Abbestellen hohe Hürden gesetzt bzw. der Prozess vergleichsweise mühsam recherchiert werden muss. Hierfür gibt es für den US-amerikanischen Markt dokumentierte Beispiele von Live Nation und Ticketmaster, einem Onlineticketversandhandel, der über eine Trickfrage ein kostenpflichtiges Abonnement mit verkaufen, das aktiv abgewählt werden muss. Wird die Checkbox nicht aktiviert, erfolgt der Kauf automatisch. Der einzige Weg zum Abbestellen des kostenpflichtigen Abos ist, ein Formular herunterzuladen, es auszudrucken, händisch auszufüllen und per Post zuzusenden.

Andere Dark Patterns zielen darauf ab, die Aufmerksamkeit der Kunden bei versteckten Kosten zu reduzieren (Misdirection) oder Preisvergleiche zu erschweren. Das Design der Webseite ist dann so ausgelegt, dass es die Aufmerksamkeit steuert, um von nachteiligen Aspekten abzulenken. Internationale Beispiele finden sich vermehrt im Bereich von Low-Cost-Airlines. Auf der Webseite können gegen ein zusätzliches Entgelt Sitzplätze ausgewählt werden. Oft ist diese Option bereits voreingestellt unter Zuweisung eines beliebigen Sitzplatzes. Die Zusatzkosten können dann nur über eine häufig schwer aufzufindende Funktion „Sitzplatzauswahl überspringen" vermieden werden. Trügerisch sind

dabei Art und Weise, wie suggeriert wird, man habe sich (kostenpflichtig und aktiv) bereits für einen Sitzplatz entschieden. Ebenso wird die Tatsache verschleiert, dass die Kosten vermieden werden können. De facto wird ein Opt-in-Prozess vorgetäuscht.

Ein weiteres Beispiel für manipulatives Webseitendesign betrifft die Erschwernis von Preisvergleichen im Onlinehandel. Fundierte (Kauf-)Entscheidungen werden so erschwert oder verhindert. Einzelhändler erreichen dies in der Regel durch die Zusammenstellung verschiedener Bündel von Waren oder Dienstleistungen. Bei dieser Art von Produktzusammenstellungen soll verhindert werden, den Stückpreis der Artikel innerhalb der Pakete ermitteln zu können. Dies war bereits in den frühen 2000er Jahren eine gängige Praxis bei Mobilfunkbetreibern.

Ähnlich funktionieren Designs, die darauf ausgelegt sind, erst spät – beispielsweise im letzten Schritt des Bestellvorgangs – einige unerwartete Kosten zu offenbaren, wie die Versandkosten. So werden etwa bei dem US-amerikanischen Blumenversand „Proflowers“ erst im fünften Schritt eines sechsstufigen Checkoutprozesses nach Eingabe der Kreditkartendaten die zusätzlichen Kosten für Lieferung und Servicegebühr dargelegt. Dabei wird ausgenutzt, dass Kunden viel Zeit für die Auswahl eines Produkts und die Dateneingabe investiert haben und daher die versteckten Kosten letztlich doch akzeptieren werden – dies möglicherweise entgegen der impliziten Erwartung, dass die Versandkosten bereits im Preis inbegriffen sind.

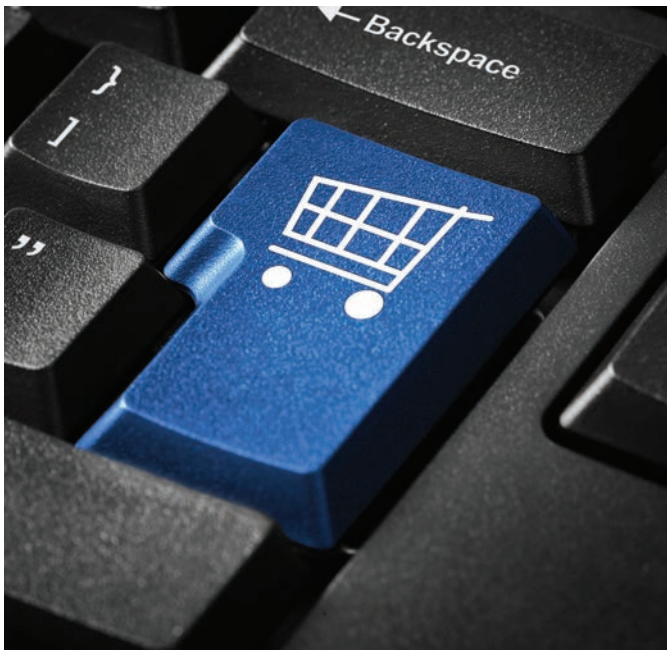
Gesellschaftliche und politische Relevanz

Das Thema hat eine hohe gesellschaftliche Relevanz, da die Nutzung des Internets im Zeitalter der Digitalisierung zur elementaren Voraussetzung gesellschaftlicher Teilhabe geworden ist. Viele Bereiche des täglichen Lebens werden durch das Internet unterstützt, beschleunigt oder erst ermöglicht, sodass durchaus von einer Abhängigkeit von diesem Medium gesprochen werden kann. Viele Internetnutzende sind insbesondere auch auf eine intuitive und leicht verständliche Nutzbarkeit der angebotenen internetbasierten Dienstleistungen angewiesen. Aus diesem Grund erhöht sich das Schadenspotenzial der Dark Patterns. Sie sind insbesondere auch aus sozialen Gesichtspunkten ungerecht, da Wissens- oder Wahrnehmungsdefizite seitens der Verbraucherinnen und Verbraucher ausgenutzt werden. Insbesondere unerfahrene Jugendliche, ältere Menschen oder bildungsferne Gruppen sind von dieser Art der Manipulation besonders betroffen.

So existieren auch Dark Patterns in der Gamesbranche (Zagal et al. 2013). Insbesondere für Kinder und Jugendliche liegen hier mögliche Risiken. Kürzlich prüfte die Stiftung Warentest (2019) 14 Spiele-Apps: Für keines der geprüften Produkte konnte eine Empfehlung ausgesprochen werden, eines wurde als im Kinderschutz bedenklich eingestuft, 13 sogar als inakzeptabel. Moniert wurden insbesondere verführerische In-App-Käufe, die schnell mit mehreren Hundert Euro zu Buche schlagen können. Laut Datenschutz-Grundverordnung müssten die Datenschutzerklärungen für derlei Dienste so formuliert sein, dass sie Kinder verstehen können. Keine der geprüften Apps erfüllt dies jedoch, so die Tester.

Aus juristischer Sicht sind die eingesetzten Mittel im Lichte des § 3 des Gesetzes gegen den unlauteren Wettbewerb (UWG) zu interpretieren und wie folgt definiert: „Geschäftliche Handlungen, die sich an Verbraucher richten oder diese erreichen, sind unlauter, wenn sie nicht der unternehmerischen Sorgfalt entsprechen und dazu geeignet sind, das wirtschaftliche Verhalten des Verbrauchers wesentlich zu beeinflussen.“ In diesem Sinne unlauter sind unter anderem besonders aggressive Verkaufsmethoden, Irreführung und Laienwerbung. Auf EU-Ebene sind grundsätzlich unzulässige Geschäftspraktiken im Anhang zu § 3 Abs. 3 UWG aufgeführt (schwarze Liste; derzeit 30 unlautere Geschäftspraktiken). Dabei untersagt Nr. 29 die „Aufforderung zur Bezahlung nicht bestellter, aber gelieferter Waren oder erbrachter Dienstleistungen“. Hierunter würden theoretisch auch Fälle des In-den-Warenkorb-Schleichens fallen – sofern dagegen erfolgreich geklagt wird. Auch die internationale Handelskammer (ICC) Deutschland (2018) spricht sich gegen den Trägheitsverkauf aus. Dennoch kann von einer hohen Dunkelziffer nichtgemeldeter Fälle ausgegangen werden. Es existieren gegenwärtig Machenschaften, die kostenpflichtige Kundenmitgliedschaften unterschieben und später Abmahnungen durch Inkassounternehmen durchführen, um Druck auszuüben (Verbraucherzentrale NRW e.V. 2019).

Möglicherweise kann auch ein Verstoß gegen die Preisauszeichnungspflicht vorliegen, wie es die Preisangabenver-



ordnung (PAngV) vorgibt. Grundpreise, das heißt Preise in Bezug auf definierte Maßeinheiten wie Liter, Kilogramm, Kubikmeter oder Quadratmeter, müssen gemäß § 2 PAngV gegenüber Verbrauchern offengelegt werden. Doch auch hier müssen Nutzende einen Verstoß gegen die Verordnung zunächst erkennen, um dagegen vorgehen zu können. Dies ist bei einer geschickten Verschleierung von Preisen möglicherweise schwierig oder gar unmöglich.

Die Verordnung (EU) 2016/679 (Datenschutz-Grundverordnung) hat mit Artikel 7 im Bereich des Erschleichens personenbezogener Daten deutliche Hürden eingezogen: So „muss der Verantwortliche nachweisen können, dass die betroffene Person in die Verarbeitung ihrer personenbezogenen Daten eingewilligt hat." Die Einwilligung muss folglich aktiv gegeben werden. Dabei wird die Nutzung bestimmter Dienste, beispielsweise Google, an die Zustimmung zu umfangreichen Bedingungen geknüpft, deren Studium mitunter Stunden dauern kann (Verbraucherzentrale NRW e.V. 2015). Insofern ist das Vorliegen einer informierten Einwilligung laut Datenschutz-Grundverordnung fragwürdig – häufig werden diese Einwilligungen vermutlich aus Zeitgründen oder mangels Alternativen gegeben, ohne genaue Kenntnis der Folgen. Auch entschied kürzlich das Oberlandesgericht Frankfurt a.M. (OLG Frankfurt, 27.6.2019 – 6 U 6/19), dass die Kopplung der Teilnahme an einem Gewinnspiel mit einer Werbeeinwilligung konform mit der Datenschutz-Grundverordnung ist.

Das Thema ist auch insofern politisch relevant, da insbesondere aus Sicht des Verbraucherschutzes regulatorische Handlungsnotwendigkeiten bestehen. Ebenso steht Dark Pattern im übergeordneten Zusammenhang mit einer allgemeinen Tendenz der technologisch gestützten Manipulation menschlichen Verhaltens. Im Unterschied zu einem durch die Nutzenden gewünschten und vor allem auch transparenten Prozess des technologischen Nudgings – wie es z.B. in Form von Fitness-Apps oder Apps zur Änderung gesundheitsschädlichen Verhaltens üblich ist – rufen Dark Patterns auf intransparente Art und Weise nachteilige und nichtintendierte Effekte hervor. Dieser Schadmechanismus ist mit jenem von Social Bots in etwa vergleichbar, die bewusst getarnt werden und vortäuschen, echte (menschliche) Nutzer zu sein, um eine Wahrnehmungs- und ggf. Verhaltensänderung herbeizuführen. Wie auch im Fall von Social Bots, ist jedoch bis dato der tatsächliche individuelle und gesellschaftliche Schaden von Dark Patterns noch nicht empirisch belegt. Ebenso schwierig dürfte das Entwickeln von technischen und politischen Strategien sein, diese einzuhegen.

In diesem Zusammenhang ergibt sich auch die Notwendigkeit, die Rahmenbedingungen der Bildungs- bzw. Ausbildungspläne von Berufen im Bereich Informatik und Webseitendesign anzupassen. Über die Konsequenzen des eigenen beruflichen Handelns finden im Rahmen der relevanten MINT-Studiengänge keine strukturierten Ethikbe-

trachtungen statt – im Gegensatz etwa zu Berufen im Bereich der Lebenswissenschaften, wo umfangreichere Richtlinien und Begleitforschungsprogramme zu ethischen, rechtlichen und sozialen Aspekten der Lebenswissenschaften (ELSI/ELSA) vorliegen. Zu entsprechenden Forschungsvorhaben an Hochschulen existieren üblicherweise Ethikkommissionen, während vergleichbar institutionalisierte Kommissionen im Bereich der Informatikforschung oder Datenwissenschaften bislang fehlen. Im Bereich der Informatik und Digitalisierung sind gegenwärtig nur temporäre Beratungsgremien installiert, wie die Datenethikkommission oder die Enquete-Kommission „Künstliche Intelligenz". Reflexionen und Betrachtungen der Auswirkungen ethisch fragwürdiger Webseitendesigns müssten verstärkt adressiert werden. So könnte sich eine Professionsethik im Bereich Informatik in Bezug auf Webseitendesign und generell in Bezug auf das Design von digitalen Mensch-Maschine-Schnittstellen noch stärker herausbilden. Ebenso könnten im positiven Sinn auszurichtende Forschungsprogramme dazu beitragen, Erkenntnisdefizite über die Wirkung und Auswirkung von Dark Patterns zu mindern sowie technologische Mittel zum Aufdecken unethischer und fragwürdiger Webseitendesigns zu entwickeln und zu implementieren. Gängige Dark Patterns könnten so künftig ggf. automatisch entdeckt werden, analog der Wirkungsweise von Spamfiltern oder Adblockertechnologien.

Schließlich könnte auch verstärkt darauf hingewirkt werden, dass unethische Designs von Webseiten im Rahmen freiwilliger Selbstverpflichtungen der Industrie eingeschränkt werden. Es könnten Best Practices mit Vorbildcharakter entwickelt werden, z.B. auch durch die Auslobung von Wettbewerbspreisen.

Mögliche vertiefte Bearbeitung des Themas

Das vorliegende Kurzprofil beinhaltet eine überblicksartige Bestandsaufnahme von Mechanismen der Dark Patterns, die für Nutzende potenziell schädlich sind. Im Rahmen einer möglichen vertieften Bearbeitung des Themas in Form einer Kurzstudie könnten auch weitere, onlinebasierte Geschäftsmodelle größerer Plattformbetreiber in den Blick genommen werden: So sind etwa bestimmte Mechanismen von Streamingportalen, wie Netflix oder Amazon Prime, auf einen potenziell süchtig machenden Massenkonsum ausgerichtet, um Abonnentinnen und Abonnenten möglichst lange zu binden. Hier werden unter anderem Elemente des Neuromarketings genutzt, um menschliches Verhalten zu beeinflussen und das Suchtpotenzial zu steigern. Zu behandeln wären etwa auch solche Aspekte, die im Kontext der anstehenden Evaluation der Datenschutz-Grundverordnung von Relevanz sind. So sieht z.B. Artikel 97 der Datenschutz-Grundverordnung vor, dass bis zum 25. Mai 2020 von der Europäischen Kommission ein „Bericht über die Bewertung und Überprüfung" der Datenschutz-Grundverordnung erfolgen soll (BMWi 2019). Die betrachteten Beispiele und gewonnenen Erkenntnisse könnten ggf. von politischer Seite dafür genutzt werden, Vorschläge für eine Ergänzung der auf EU-Ebene grundsätzlich unzulässigen Geschäftspraktiken, aufgeführt im Anhang zu § 3 Abs. 3 UWG, zu machen.

Ebenso könnten Erkenntnisse einer vertieften Bearbeitung in die laufenden Arbeiten von Standardisierungsgremien (DIN; IEEE) eingespeist bzw. von diesen aufgegriffen werden. Die Ergebnisse können sowohl Empfehlungscharakter haben als auch bereits existierende Selbstverpflichtungen von Internetunternehmen ergänzen oder für die Erstellung von Designethikhandreichungen genutzt werden. Es könnten ebenfalls internationale Beispiele betrachtet werden, da sich die Regulierung onlinebasierter Geschäftspraktiken länderspezifisch unterscheidet.

Die Herausforderung besteht insgesamt darin, Hinweise für eine umsichtige Regulierung von Dark Patterns zu generieren, zugleich jedoch eine Überregulierung zu vermeiden, da ansonsten auch sinnvolle Features von Webseiten entfallen würden (Thien Hang Nguyen/Kissner 2019). Gerade jene Designmechanismen von Dark Patterns, die die Aufmerksamkeit der Nutzerinnen und Nutzer steuern, dienen im Rahmen ethisch designter Nutzerschnittstellen dazu, Informationen schneller und möglichst barrierefrei auffindbar zu machen sowie Komplexität zu reduzieren. Es ist darauf zu achten, dass durch eine Überregulierung nicht die Softwareergonomie leidet, was zu Komforteinbußen führen oder gar die praktische Umsetzung der Verordnung zur Schaffung barrierefreier Informationstechnik nach dem Behindertengleichstellungsgesetz (Barrierefreie-Informationstechnik-Verordnung – BITV 2.0) konterkarieren würde. Das generelle Ziel liegt darin, die spezifisch negativen Praktiken – eben die Dark Patterns – zu identifizieren und ggf. unterbinden zu können.

Literatur

- BMWi (Bundesministerium für Wirschaft und Energie) (2019): Europäische Datenschutz-Grundverordnung. Berlin, https://www.bmwi.de/Redaktion/DE/Artikel/Digitale-Welt/europaeische-datenschutzgrundverordnung.html (23.9.2019)
- Internationale Handelskammer (ICC) Deutschland (2018): ICC Advertising and Marketing Communications Code. Building Consumer Trust through responsible Marketing. https://cms.iccwbo.org/content/uploads/sites/3/2018/09/icc-advertising-and-marketing-communications-code-int.pdf (19.9.2019)
- Proschofsky, A. (2019): Stressfaktor: Wie Booking.com und Co die Nutzer zu unüberlegten Buchungen bringen. STANDARD, 23.9.2019, https://www.derstandard.at/story/2000108894531/stressfaktor-wie-bookingcom-und-co-die-nutzer-zu-unueberlegten-buchungen (26.9.2019)
- Stiftung Warentest (2019): Spiele-Apps im Test – Alles andere als kindgerecht. https://www.test.de/Spiele-Apps-im-Test-Alles-andere-als-kindgerecht-5197290-0/ (24.9.2019)
- Thien Hang Nguyen, S.; Kissner, L. (2019): When Politicians Play Web Designers. WIRED, 25.9.2019, https://www.wired.com/story/when-politicians-play-web-designers/ (30.9.2019)
- Thurrott, P. (2016): Upgradegate: Microsoft's Upgrade Deceptions Are Undermining Windows 10 (Updated). https://www.thurrott.com/windows/windows-10/67367/upgradegate-microsofts-upgrade-deceptions-undermining-windows-10 (19.9.2019)
- Verbraucherzentrale NRW e. V. (2015): Google fordert Zustimmung zum Datenschutz. https://www.verbraucherzentrale.de/wissen/digitale-welt/datenschutz/google-fordert-zustimmung-zum-datenschutz-12309 (23.9.2019)

- Verbraucherzentrale NRW e. V. (2017): Klickfalle bei E-Mail-Anbietern: So kommen Sie aus den Verträgen rauS.https://www.verbraucherzentrale.de/wissen/digitale-welt/onlinedienste/klickfalle-bei-emailanbietern-so-kommen-sie-aus-den-vertraegen-raus-13614 (9.10.2019)
- Verbraucherzentrale NRW e. V. (2019): „Probenheld“: Abofallen statt Probenfreuden. https://www.verbraucherzentrale.de/aktuelle-meldungen/digitale-welt/probenheld-abofallen-statt-probenfreuden-35536 (23.9.2019)
- Zagal, J. P.; Björk, S.; Lewis, C. (2013): Dark Patterns in the Design of Games. Foundations of Digital Games conference, 14.–17.5.2013, Chania, http://www.fdg2013.org/program/papers/paper06_zagal_etal.pdf (9.10.2019)

Das Horizon-Scanning ist Teil des methodischen Spektrums der Technikfolgenabschätzung im TAB.

Horizon SCANNING

Mittels Horizon-Scanning werden wissenschaftlich-technische Trends und sozio-ökonomische Entwicklungen in frühen Entwicklungsstadien beobachtet und in den Kontext gesellschaftlicher Debatten eingeordnet. So sollen Innovationssignale möglichst früh erfasst und ihre technologischen, ökonomischen, ökologischen, sozialen und politischen Veränderungspotenziale beschrieben werden. Ziel des Horizon-Scannings ist es, einen Beitrag zur forschungs- und innovationspolitischen Orientierung und Meinungsbildung des Ausschusses für Bildung, Forschung und Technikfolgenabschätzung zu leisten.

In der praktischen Realisierung wird das Horizon-Scanning als Kombination softwaregestützter Such- und Analyseschritte und eines expertenbasierten Validierungs- und Bewertungsprozesses durchgeführt.

Herausgeber: Büro für Technikfolgen-Abschätzung beim Deutschen Bundestag (TAB)

Gestaltung: VDI/VDE Innovation + Technik GmbH

Bildnachweise: © artinspiring/AdobeStock (S.1), nicescene/AdobeStock (S.2), Alex Rühl/AdobeStock (S.3), Coloures-Pic/AdobeStock (S.4), samuel/AdobeStock (S.5), Mymemo/AdobeStock (S.6)

ISSN-Internet: 2629-2874