Diginomics Working Paper

Research Group Diginomics
Digitalization - Economy - Society

Digital Dark Nudges

Lars Hornuf, Sonja Mangold

April 2022 No. 0012

Universität Bremen

Impressum:

Diginomics Working Paper

ISSN: 2701-6307

DOI: http://dx.doi.org/10.26092/elib/1466

Published by:
Universität Bremen, Diginomics Research Group, Max-von-Laue-Straße 1, 28359 Bremen, Germany

Editor:
Prof. Dr. Lars Hornuf
Phone: +49(0)421 218 66820
E-mail: hornuf@uni-bremen.de

https://www.uni-bremen.de/graduiertengruppe-diginomics/forschung/diginomics-working-paper

This working paper will appear in L. Hornuf (Ed.), *Diginomics Research Perspectives: The Role of Digitalization in Business and Society*. Cham: Springer International Publishing.

Digital Dark Nudges

Lars Hornuf and Sonja Mangold

Abstract

Manipulative product and interface designs known as digital "dark nudges" have become a common phenomenon in the digital economy. This chapter investigates the behavioral science background and the main problem areas of such unethical online business practices. We also show the limits of the existing statutory framework for combating digital dark nudges. The chapter concludes by discussing potential private and statutory remedies to address dark nudges in the digital economy.

5.1 Introduction

Websites and apps with fraudulent designs that lead users to inadvertently commit to contracts and subscriptions or to divulge more personal data than they actually want are widespread in the digital economy. Companies are increasingly resorting to dubious design practices such as manipulative coloring or font size of buttons and confusing language in order to increase profits and to obtain and monetize as much user data as possible. Such business tactics, which are often at the expense of consumers and direct competitors, have been termed by academics as digital "dark nudges" and "dark patterns" (Brignull 2010, 2013; Luguri & Strahilevitz 2021; Reisch 2020). A uniform definition of manipulative digital designs does not yet exist (Martini et al. 2021). According to the pioneering definition by Brignull (2013), digital dark nudges are the "dark side of design" that have been crafted "with great attention to detail, and a solid understanding of human psychology, to trick users into do things they wouldn't otherwise have done."

5.1.1 Manifestations of Digital Dark Nudges

There is a great deal of variation in the use of digital dark nudges. Based on the available literature (Gray et al. 2018; Luguri & Strahilevitz 2021; Martini et al. 2021; Mathur et al. 2019), five archetypes can be distinguished. The first is *pressure* to take or not to take a certain action. This includes repeated aggressive inquiries even though users have already declared their intent – also known as "nagging" – which are often accompanied by indications of an alleged scarcity of goods. Another example is known as "confirmshaming," for example, where rejection buttons are formulated to embarrass users into acceptance. The second type is

operational constraint, in which the user actually has no decision-making option or an alternative decision is linked to undesirable conditions. An example of this practice is known as "forced enrollment," in which the use of a service is made dependent on the user accepting further conditions that are not required for the provision of the service. "Forced continuity" is another common practice, in which free or low-cost trial subscriptions are automatically renewed, but for a fee or at an increased price. Third, *obstruction* seeks to discourage users from performing certain actions by placing obstacles in their path. This includes pre-selecting checkboxes to the least privacy-friendly options. Another example is "click fatigue," in which the click paths to various options are designed with different lengths so that users often choose the simpler option and, for example, accept all cookies. A "roach motel" is a strategy whereby signing up or subscribing is much easier than canceling. Fourth, *sneaking* forces users to make additional purchases of goods or services without initially realizing it, for example when an additional item ends up in the shopping cart unintentionally. Similarly, with hidden subscriptions, users are signed up for a recurring fee under the guise of a one-time fee or a free trial. Fifth, *misleading* uses graphic design to divert attention from certain information or to subvert users' usual design expectations. One example is trick questions (e.g., using a double negative) that lead to consumers no longer recognizing the significance of their choices. Also common are misdirection strategies whereby conspicuous graphic elements distract from the content.




Pressure to (not) take a certain action	**Operational Constraint** Users actually have no decision-making option	**Obstruction** tries to dissuade users from certain actions by placing obstacles in their way.	**Sneaking** imposes additional purchases of goods or services without initially noticing	**Misleading** uses graphic design to divert attention from certain information
Includes: Nagging Confirmshaming	**Includes:** Forced Enrollment Forced Continuity	**Includes:** Preselection Click Fatigue Roach Motel	**Includes:** Sneak in the shopping cart Hidden Subscription	**Includes:** Trick questions Misdirection

Fig. 5.1 *Five archetypes of digital dark nudging strategies (based on Martini et al. 2021)*

5.1.2 Behavioral Science Background

One of the fundamental questions of legal theory is what assumptions about human behavior should be made (Eidenmüller 2011). The legislature may assume that citizens are

fundamentally rational in pursuing their subjective goals and interests. If so, digital dark nudges would not be effective and business strategies built on these practices would be essentially worthless. Behavioral science has nevertheless shown that people systematically make mistakes and act predictably irrationally in certain situations (Ariely 2010; Kahneman 2012). Therefore, the law must intervene and protect consumers from business practices such as digital dark nudges.

Nudges are broadly defined as mechanisms that aim to steer human behavior in a certain direction without prohibiting certain decision options and without fundamentally changing existing economic incentives (Thaler & Sunstein 2009). Hence, nudges have often been viewed by behavioral and legal scholars as something positive that helps people make better decisions. Most prominently, Thaler and Sunstein (2009) put the concept of nudging on the global political agenda, arguing that a choice architecture cannot be avoided and therefore nudges should be implemented "that are most likely to help and least likely to inflict harm" (p. 74).

Digital dark nudging strategies do not have such positive intentions. What they have in common with positive nudges is that they use behavioral knowledge about human decision-making. Psychologists and particularly behavioral economists have discovered a veritable zoo of different behavioral anomalies that can be exploited. Scholars such as Todd and Gigerenzer (2007) have shown that heuristics, which are simple decision algorithms or mental shortcuts, can work very efficiently in specific environments and enable humans to make better decisions. They refer to the *recognition heuristic* as one such positive decision support system. For example, if people recognize one tennis player but not the other, then the recognized one is the one more likely to win (Gigerenzer 2007). However, an extensive literature also shows that humans suffer from biases in their decision-making. For example, default bias refers to the tendency for a human to generally accept the default option in a strategic interaction, potentially because switching involves costs and cognitive effort (Altman 2017). Amazon has used default bias in their business practices by setting "Subscribe and Save" as the default for some products, with the goal of luring customers into this option. Knowledge about behavioral science has hence become a decisive source of competitive advantage in the digital economy (Luca & Bazerman 2020).

5.2 Driving Factors and Risk Potential

Numerous studies have shown that dark nudges are used in a wide variety of industries and have a considerable control effect on the behavior of internet users (Luguri & Strahilevitz 2021; Mathur et al. 2019; Utz et al. 2019). As a result of fierce competitive pressure in the global digital economy, companies are increasingly investing in tricky interface designs in order to increase user numbers and to raise profit margins (Rieger & Sinders 2020). With the help of field experiments, which primarily take place in the form of A/B testing,[1] the effects of design variants on user behavior are examined and the respective designs are optimized (Luca & Bazerman 2020). Big tech companies such as Alibaba, Amazon, Facebook and Google that

[1] A/B testing is a method in which two variants of an app or website are tested and compared. The goal is usually to evoke or increase a specific user action.

have billions of users have almost inexhaustible possibilities to test which designs have the desired effect on consumer behavior. But even smaller companies can buy huge datasets from third party providers to exploit the individual weaknesses of users (Perlroth 2021). Big data analytics also open up new and dangerous potential for creating and applying personalized digital dark nudges (Reisch 2020; Martini et al. 2021; Weinzierl 2020).

Such designs can portend increased risks for vulnerable consumer groups. The costs of fraudulently solicited purchases and subscriptions hit socially disadvantaged consumers particularly hard. Older "digital immigrants" are also at risk of being manipulated more frequently and effectively. Similarly, inexperienced users such as children and adolescents may be easily controlled, deceived, and seduced into unwanted actions such as sensitive data disclosure (Bogenstahl 2019).

Manipulative design practices pose challenges for the legal system, as well as blunting the efforts of benevolent companies in the digital economy.[2] Companies that use digital dark nudges may violate data protection law, can be prosecuted under competition law, or might even risk criminal prosecution for fraud. Often, however, misleading designs operate in a gray area that is legally difficult to grasp, which is discussed in more detail below. Deceptive companies are constantly using new and increasingly sophisticated digital dark nudges, which makes it difficult for the legislature to control this phenomenon in a problem-oriented manner. Moreover, it is often much more difficult for consumers and competitors to enforce the law in cross-border digital markets (see in general Calliess 2006; with regard to digital dark nudges Reisch 2020).

5.3 Relevant Problem Areas

5.3.1 Case 1: Manipulative Design of Cookie Banners

One of the most common examples of digital dark nudges involves design tricks related to cookie banners. The purpose of cookies is to store information related to a website locally on a user's digital device for a certain period of time. During the next visit the information is transmitted back to the server of the company the user wishes to engage with. Cookies thus enable companies to individualize their websites for users by authenticating them when they return to the website. Since 2002, the Privacy and Electronic Communications Directive (also known as the ePrivacy Directive or, more colloquially, the "cookie directive") has regulated minimum standards for cookies in EU member states. After its amendment in 2009, the directive has made cookies subject to prior consent, which has led to an increasing use of dark nudges to get customers to consent to cookies (Hausner & Gertz 2021; Utz et al. 2019). Through manipulative design variations, companies use deceptive consent queries to persuade consumers to agree to cookie settings that will disclose as much personal data as possible to create comprehensive individual user profiles, for example, for targeted advertising purposes. In other business models, user profiles are created to calculate default probabilities

[2] Manipulative designs by private actors often aim at excessive data collection. Klein et al. (2022) discuss privacy concerns in digital marketing and Kinra et al. (2022) analyze data privacy challenges of social media analytics. Karpa et al. (2022) study data privacy risks caused by authoritarian states.

and make credit decisions (Dorfleitner et al. 2021). Problematic design practices with cookie notices occur in various forms, including the graphic design of buttons, hidden privacy-friendly options, or through specific default settings.

5.3.1.1 Practical Examples

Dark nudges in cookie banners often appear in the form of manipulative color designs of individual buttons. Figure 2 shows a typical example of such tricky design variants.[3] The "accept all" button graphically clearly stands out with a colored background to encourage the user to agree to comprehensive web tracking. In contrast, clearly upstaging the pale gray "reject" button. This type of influence is a dark nudge in the form of *misleading*. By choosing based on different colors, consumers can be tempted to disclose more data than they presumably want.

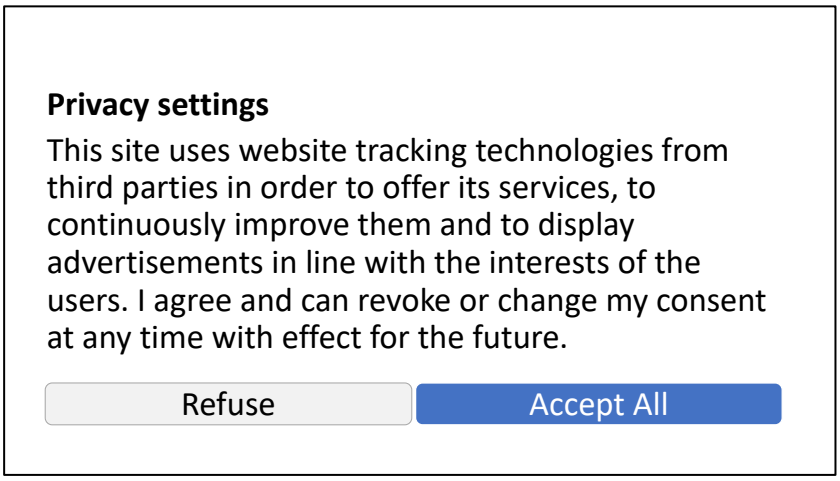

Fig. 5.2 *Digital dark nudging in the form of deceptive color design*

Figure 3 shows another common variant of the manipulative design of cookie banners. The provider makes the unrestricted use of its website conditional on the granting of consent for web tracking. In this way, users are effectively forced to consent to the use of cookies. This example is a conditional dark nudge that can be classified in the category of operational constraint.

[3] All figures are based on website designs and privacy practices by real companies in 2021.

Fig. 5.3 *Digital dark nudging in the form of operational constraint*

An example of obstruction designs is the use of *click fatigue*, which makes the refusal of consent to web tracking dependent on further, cumbersome actions. Such a case is shown in Figure 4. The website provider moves the rejection option to a settings menu, whereby users on the first level cannot see how many steps are necessary to ultimately refuse their consent. The desire of users to visit the website without interruption regularly leads to their consent to web tracking instead of clicking on the “settings” button.

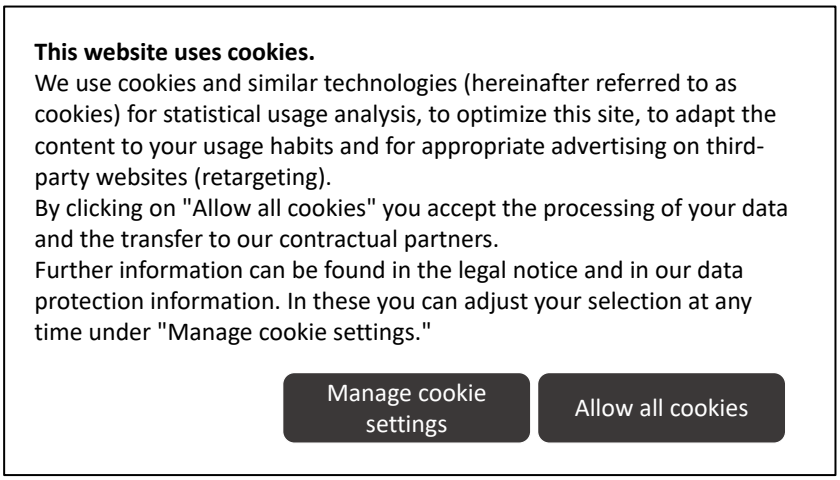

Fig. 5.4 *Digital dark nudging in the form of click fatigue*

Studies have shown that big tech companies often use several digital dark nudges at the same time, for example, by using a combination of manipulative color design, misleading language and hiding privacy-friendly options to urge users to accept the lowest possible data privacy settings (Norwegian Consumer Council 2018). Facebook currently encourages users to accept web tracking for advertising purposes by highlighting the “accept all” button and uses click fatigue by presenting the alternative as a commitment to “manage” settings.

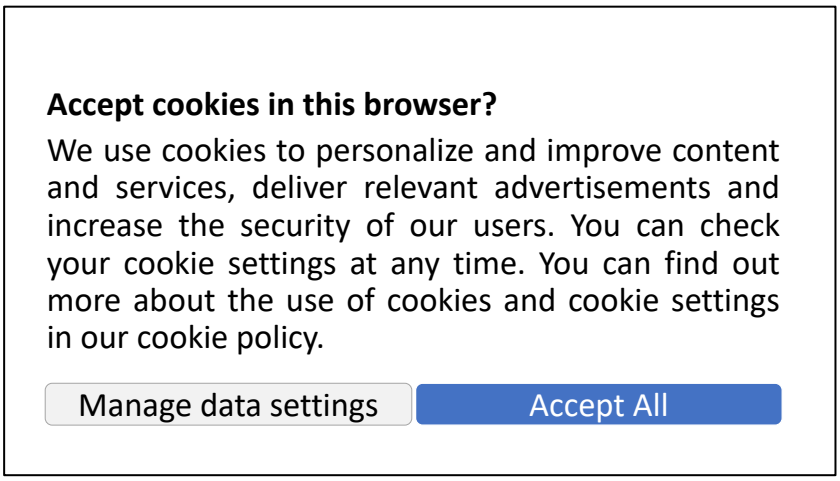

Fig. 5.5 *Digital dark nudging in the form of manipulative color design and click fatigue*

5.3.1.2 Legal Aspects and Gaps in Privacy Protection

Digital dark nudges in cookie banners can be legally problematic, especially from a data privacy perspective.[4] European and German privacy law[5] generally require that users give their voluntary, specific, informed consent to the use of tracking and advertising cookies. The requirements for consent are laid down in the General Data Protection Regulation (GDPR)[6], which became binding in all EU member states in May 2018. If there is no valid consent, the use of cookies is illegal. It can be argued that data protection law currently prohibits some forms of dark digital nudges in cookie banners, but by no means covers all of them (Loy & Baumgartner 2021; Sesing 2021). European and German jurisprudence[7] recently put a stop to obstruction and preselection nudges in particular. Consequently, the website visitor's assent to the use of cookies through pre-selected check boxes is not permitted – consent must be given actively and expressly.

The question of whether and to what extent it is permissible to induce users to give their consent by different button designs is legally controversial. According to the prevailing view of the literature, highlighting the "accept all" or "reject" buttons in a different color, as exemplified in Figure 2, does not lead to such a strong steering effect that it would negate voluntary consent (Loy & Baumgartner 2021). The question of whether it is permissible to make the unrestricted use of a website dependent on consent to tracking has also not been clearly answered (Sesing 2021). The example of conditional nudging shown in Figure 3 is therefore in a legal gray area. Click fatigue strategies that make the rejection of all cookies more cumbersome than accepting all cookies are widely viewed as illegal in case law and literature (Loy & Baumgartner 2021). The examples of digital dark nudges illustrated in Figures 4 and 5 should therefore be impermissible.

---

[4] Illegal cookie practices can also have consequences under competition law.

[5] See Art. 5 (3) ePrivacy Directive; § 15 (3) Telemedia Act and the pending Section 25 (1) Telecommunications Telemedia Data Protection Act.

[6] See Art. 4 No.11, Art. 7 GDPR.

[7] See European Court of Justice (ECJ) (2019), Case C-673/17 ("Planet49"); Federal Court of Justice (BGH) (2020), case file number I ZR 7/16.

It can be argued that data protection law *de lege lata* only prohibits some forms of manipulative designs. In order to close legal protection gaps, legal scholars have called for the creation of standardized specifications for the design of cookie banners (Sesing 2021). Comparable legal requirements already exist in European consumer protection law with regard to consumers' revocation rights. The legal equivalence is argued in the literature, according to which it should be just as easy for users to withhold their consent as it is to give it (Sesing 2021). This is intended to put a stop to obstruction designs in the form of click fatigue strategies. However, in view of the diverse manifestations of digital dark nudges in cookie banners, it is questionable whether individual legal amendments are sufficient. It must also be taken into account that existing regulations are often not complied with. The German consumer protection authorities recently warned numerous companies about impermissible cookie consent management.[8] In the summer of 2021, the non-governmental organization None of Your Business, led by the Austrian data protection activist Max Schrems, filed complaints with data protection authorities against digital dark nudges in cookie banners.[9] Hence there are significant legal and practical gaps in privacy protection that remain to be resolved.

5.3.2 Case 2: Subscription Traps

The second type of digital dark nudging we examine is subscription traps.[10] Subscription traps lead consumers to unwanted enrollment or renewal of subscriptions through manipulative design techniques. The forms of such subscription traps on the internet are diverse (Gray et al. 2018; Martini et al. 2021; Rieger & Sinders 2020). For example, users are tempted to take out a subscription because only then can they use the service or certain functions. These *forced enrollment* strategies fall into the category of operational constraints*. Forced continuity* nudges are also common. After a trial period, an annual membership is automatically commenced or a subscription is automatically extended. Another business practice is to make the termination of a membership more difficult by obscuring or concealing such functions. This is another example of the roach motel described above, whereby it is much easier for users to take out a subscription than to cancel it. Companies may also try to trick consumers into automatically subscribing to services through deceptive designs. This type of digital dark nudging is known as *hidden subscription.*

5.3.2.1 Practical Examples

This section presents three illustrated cases of subscription tricks related to digital dark nudges. In the first case, as exemplified in Figure 6, the company uses a "freemium" business model to acquire business customers. The basic product is offered free of charge, while the full product and extended functions are only available for a fee. Users also typically experience

[8] More information on these topics can be found here: https://www.vzbv.de/pressemitteilungen/jedes-zehnte-cookie-banner-ist-klar-rechtswidrig (last accessed on November 10, 2021).
[9] For more detail, see: https://noyb.eu/de/noyb-reicht-422-formelle-dsgvo-beschwerden-gegen-cookie-banner-wahnsinn-ein (last accessed on November 10, 2021).
[10] According to the consumer advice center in Bremen, most of the complaints from consumers in connection with digital dark nudges – in addition to manipulative cookie designs – concern subscription tricks and traps.

payment barriers for certain services. In this way, users are seduced into upgrading from the free version to a paid subscription. This strategy can be classified as digital dark nudging in the form of forced enrollment.

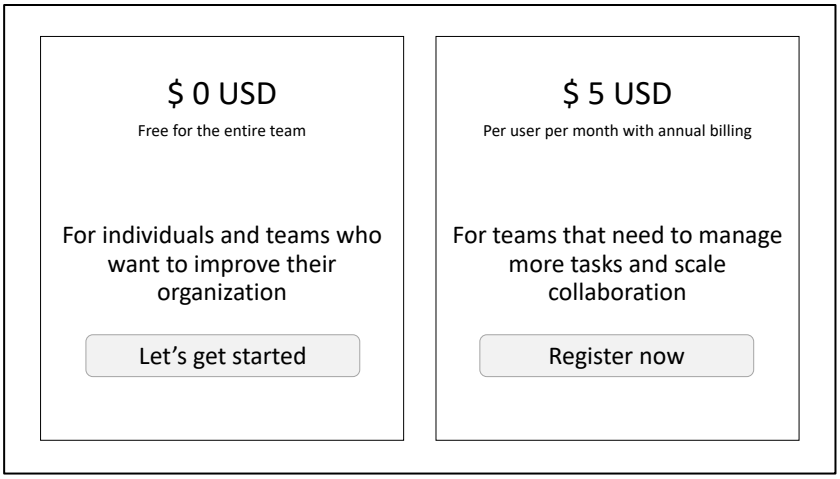

Fig. 5.6 *Subscription trick in the form of forced enrollment*

In the second case, exemplified in Figure 7, the bold and large highlighted website design promises a free trial subscription. If you click on the "contract details" below in small print you will find out that the subscription is automatically converted into an annual subscription, provided that users do not object in writing up to seven days before the end of the trial phase. The company is trying to increase sales by taking advantage of availability bias and the expected non-timely cancellation of membership by consumers. This strategy is an example of digital dark nudging in the form of *forced continuity*. Alternatively, highlighting the cost-free nature of the trial subscription compared to the costs incurred later in small letters can be regarded as a *hidden subscription* strategy.

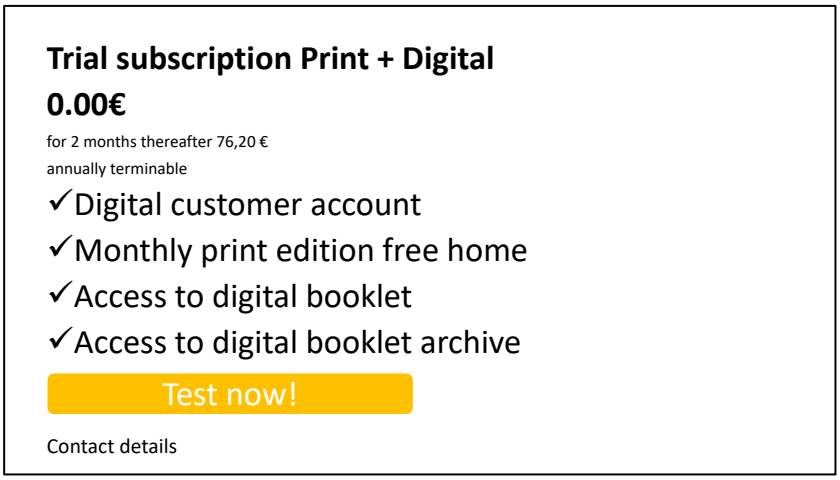

Fig. 5.7 *Subscription trick in the form of forced continuity and hidden subscription*

In the third case, as exemplified in Figure 8, the termination of a subscription is made more difficult by the company, which does not offer a termination option on the website. Instead, it asks the customer to first contact customer support via telephone. This is another example of a subscription trap in the form of forced continuity.

Fig. 5.8 *Subscription trick in the form of forced continuity*

5.3.2.2 Legal Protection Instruments and Protection Gaps

Subscription traps on the internet are pertinent to several areas of law. In particular, consumer law, general contract law, and fair-trading law put a stop to the corresponding strategies of manipulative influence on consumers by companies, at least in part (Martini et al. 2021). In the event of an act of deception, a criminal liability for fraud[11] can be triggered. This is the case, for example, when the design of a website intentionally conceals the fact that a user is entering into a paid subscription[12] and offers the possibility of penalties in the form of hidden subscription strategies under certain circumstances.

A consumer protection instrument that can also come into play relates to rights of withdrawal[13]. Rights of withdrawal are not specifically directed against digital dark nudging, but they do allow consumers to nullify a contract that has been entered into under the influence of deceptive design strategies. The right of withdrawal is particularly relevant for distance contracts[14]. Accordingly, consumers in online trading are entitled to revoke contracts within a certain period without giving reasons. However, there is doubt in the literature whether existing rights of withdrawal are used in practice (Martini et al. 2021; Rieger & Sinders 2020). Subtle tricky design practices are often not noticed or are simply accepted by consumers.

Subscription traps in which subscriptions or trial periods are automatically extended for a fee without the consumer being transparently informed during the ordering process are

[11] Section 263 of the Criminal Code (Strafgesetzbuch)
[12] See also BGH, judgment of March 5, 2014 – case file number 2 StR 616/12.
[13] Section 355 of the German Civil Code (Bürgerliches Gesetzbuch, BGB).
[14] See Section 312 c, 312 g BGB.

specifically addressed by information obligations under consumer law[15]. According to the so-called “button solution”[16], the customer must always confirm online orders with a button that does not contain anything other than the words “order with obligation to pay” or another clear formulation. If the labeling requirements are not complied with, no contract will be formed[17]. Case law has interpreted the provision strictly[18]. For example, the phrase "test now for free" was considered insufficient if the first month of a contract is free but a contractual relationship that is subject to a fee follows and the only way to prevent this from coming about is by canceling the contract. The case of forced continuity nudging, which we have exemplified in Figure 7, can thus be classified as legally problematic.

Another lever against subscription tricks is the obligation for companies to set up a cancellation button[19], which is provided for in a Germain law regarding fair consumer contracts that is scheduled to become binding at the end of May 2022[20]. According to this law, a termination button must be available on the website in the case of online-subscriptions, and must be labeled with the words "terminate contracts here" or an alternative, unequivocal formulation[21]. This reduces the hurdles for consumers to give notice of termination. In this way, forced continuity strategies that make cancellation of subscriptions difficult, as shown in Figure 8, can be counteracted.

The general contractual instruments of contestation[22] and *culpa in contrahendo*[23] also offer certain protections against influencing tactics by companies in connection with subscription traps. However, here too there is the problem, mentioned above, that consumers often do not become aware of or are indifferent to subtle digital dark nudging and therefore waive the exercise of their rights.

Subscription traps in the context of digital dark nudging can also be impermissible from the point of view of unfair competition law (Martini et al. 2021). For example, hidden subscription tricks may violate No. 21 of the Annex to Section 3 (3) of the Act Against Unfair Competition (*Gesetz gegen den unlauteren Wettbewerb*, UWG). Accordingly, the offer of a product or service must not be indicated as free or similar if costs are still to be borne. Roach motel cases in which it is much easier for users to take out a subscription than to cancel may not be allowed under German law as they constitute an "aggressive business act"[24]. Accordingly, it is forbidden for companies to create obstacles that prevent consumers from exercising their contractual rights such as termination rights. Subscriptions and continued subscriptions obtained through digital dark nudging can also violate the prohibitions of misleading under fair trading

[15] Section 312 j (2) seq. BGB.
[16] Section 312 (3) BGB.
[17] Section 312 j (4) BGB, cf. Weiss 2013.
[18] See, for example, Munich Regional Court I, decision of June 11, 2013 - 33 O 12678/13.
[19] See Section 312 k BGB.
[20] Act for Fair Consumer Contracts of 10 August 2021, Federal Law Gazette Volume 2021 Part 1 No. 53, 3433 ff.
[21] Section 312 k (2) BGB.
[22] Sections 119, 123 BGB.
[23] Sections 280 (1), 311 (2), 241 (2) BGB.
[24] Cf. Section 4a (2) no. 4 UWG.

law[25]. Consumer associations have already successfully taken legal action against competition violations in connection with internet subscription traps[26].

In summary, it is evident that existing laws only cover individual cases of digital dark nudging in the context of subscription tricks. Specific consumer protection norms still have weaknesses in factual terms of enforcement (Spindler et al. 2015). Additional legislative actions seem warranted.

5.4 Overcoming Digital Dark Nudging

In the following section we take a brief look at current regulatory approaches to combat digital dark nudging. Finally, we shortly discuss which measures could be suitable and effective to curb the problem of manipulative design tricks.

5.4.1 State and Private Regulatory Responses

In Germany there is currently no specific law to combat digital dark nudging. A first comprehensive proposal to prohibit companies from using manipulative website designs arose in the USA in 2019 with the "Deceptive Experiences to Online Users Reduction Act" (DETOUR Act).[27] The topic is nevertheless increasingly moving into the focus of German and European legislators. In its current consumer agenda,[28] the European Commission has expressly declared its commitment to fighting manipulative design practices in the digital economy. The Council of the European Union recently called for targeted improvements against digital dark nudging[29] as part of the planned comprehensive EU regulatory package for online platforms.[30]

Calls for specific improvements, particularly in consumer and fair-trading law, have become louder in the public discourse (Bogenstahl 2019). Antitrust law is seen as a possible lever to effectively counter the use of manipulative design tactics by powerful tech companies (Day & Stemler 2020). Some voices in the literature even suggest the introduction of legal limits and transparency requirements with regard to methods such as A/B tests, which make digital dark nudging effective (Martini et al. 2021). However, legal limits to A/B tests raise the question of what the correct default design should be in each case (Luca and Bazerman 2020) and whether nudges should not be used for consumers' benefit (Sunstein 2015).

---

[25] See Sections 5, 5a UWG.

[26] See, for example, higher regional court (OLG) Koblenz, ruling of December 22, 2010 - 9 U 610/10.

[27] More information can be found at: https://www.congress.gov/bill/116th-congress/senate-bill/1084/text (last accessed on November 17, 2021).

[28] See European Commission, Communication from the Commission to the European Parliament and the Council of 13th November 2020, New Consumer Agenda, COM(2020) 696 final.

[29] See for more information: https://marketresearchtelecast.com/dark-patterns-eu-countries-want-to-ban-psychological-tricks-with-the-digital-services-act/204974/ (last accessed on November 18, 2021).

[30] The proposed regulation includes the "Digital Services Act" (DSA) and the "Digital Markets Act" (DMA). The regulations include liability rules and transparency requirements for online platforms (cf. Gielen & Uphues 2021). While the DSA applies to all providers, the DMA addresses big, powerful platforms.

It is also questionable whether legal amendments are sufficient to master the problem of deceptive design tactics in the digital economy. Companies are constantly using new and increasingly sophisticated forms of digital dark nudges. In doing so, legal gray areas are often used that the legislature has not provided for. Statutory law often lags behind rapidly changing economic and technical developments. In addition, there are legal enforcement difficulties for consumers, especially if the company is based outside of Europe. The power and information asymmetry between companies and consumers, which has served as justification for active consumer protection policy within the national framework, is especially problematic in the cross-border digital economy (Adam & Micklitz 2017).

Against this background, it is worthwhile to consider complementary strategies of private self-regulation and ethical self-restraint in the digital economy. The first initiatives have already been implemented. For example, with the Advertising and Marketing Communications Code,[31] the International Chamber of Commerce created a globally applicable self-regulatory framework designed to protect consumers from unethical digital marketing practices and excessive data collection. The Interactive Advertising Bureau's Europe Transparency & Consent Framework,[32] a standard for the digital advertising industry, aims to promote global compliance with consumer data protection regulations in accordance with the GDPR and the ePrivacy Directive. The US Association for Computing Machinery (ACM) has also taken on the topic of digital dark nudging and formulated professional ethical standards in the field of IT with the ACM Code of Ethics.[33]

In addition to self-binding activities of the digital economy, rulemaking by public–private standardization bodies can help to find problem-specific solutions against digital dark nudging (Bogenstahl 2019). For example, the International Organization for Standardization has created the ISO 9241 norm, which has been adopted in Germany as DIN EN ISO 9241, and which contains quality requirements and guidance for user-friendly user experience and user interface design.[34]

5.4.2 Outlook

We have shown in this chapter that digital dark nudging has become a significant and growing problem in the internet economy. Companies in numerous industries use manipulative design tactics to suggestively influence consumers and thereby increase profits. The legislature has already taken first steps to better protect consumers and internet users. In view of increasingly dynamic economic and technical development, mere prohibitions and legal measures often fall short. Proactive, more comprehensive strategies therefore appear to be indicated to counter consumer-hostile practices in the digital world. These should include problem-related self-regulation approaches in digital industry. In addition, ethical aspects should be more

[31] Online available at: https://iccwbo.org/content/uploads/sites/3/2020/03/icc-advertising-and-marketing-communications-code-german-final.pdf (last accessed on November 18, 2021).
[32] More information is available at: https://iabeurope.eu/transparency-consent-framework/ (last accessed on November 18, 2021).
[33] Available online at: https://www.acm.org/code-of-ethics (last accessed on November 18, 2021).
[34] For more information, see: https://www.iso.org/standard/60476.html (last accessed on November 18, 2021).

closely integrated into education and training for professions in the field of IT and web design (Bogenstahl 2019). Civil society organizations such as non-governmental organizations and consumer associations can increase public pressure and thus help curb fraudulent design practices by companies. Further research is nevertheless required in order to gain better knowledge about the effectiveness of tailor-made law in relation to digital dark nudging.

Literature

Adam, L., & Micklitz, H. W. (2017). Verbraucher und Online- Plattformen. In Micklitz, H.W., Reisch, L. A., Joost, G., & Zander-Hayat, H. (Eds.). *Verbraucherrecht 2.0. – Verbraucher in der digitalen Welt*, pp. 45–102. Nomos.

Altman, M. (2017). Aspects of smart decision-making. *Handbook of behavioural economics and smart decision-making*, 155–156. Edward Elgar Publishing.

Ariely, D. (2010). *Predictably irrational: The hidden forces that shape our decisions*. Harper Collins Publishers.

Bogenstahl, C. (2019). *Dark patterns – Mechanismen (be)trügerischen Internet designs*. Retrieved November 10, 2021, from https://www.tab-beim-bundestag.de/de/pdf/publikationen/themenprofile/Themenkurzprofil-030.pdf

Brignull, H. (2010). *Dark patterns: Dirty tricks designers use to make people do stuff*. Retrieved November 10, 2021, from https://90percentofeverything.com/2010/07/08/dark-patterns-dirty-tricks-designers-use-to-make-people-do-stuff/index.html

Brignull, H. (2013). *Dark Patterns: inside the interfaces designed to trick you.* Retrieved February 7, 2022, from https://www.theverge.com/2013/8/29/4640308/dark-patterns-inside-the-interfaces-designed-to-trick-you

Calliess, G.-P. (2006). *Grenzüberschreitende Verbraucherverträge*. Mohr Siebeck.

Day, G., & Stemler, A. (2020). Are dark patterns anticompetitive? *Alabama Law Review*, 72(1), 1–46.

Dorfleitner, G., Hornuf, L., & Kreppmaier, J. (2021). Promise not fulfilled: Fintech data privacy, and the GDPR. *CESifo Working Paper No. 9359*. https://ssrn.com/abstract=3950094

Eidenmüller, H. (2011). Liberaler Paternalismus. *Juristen Zeitung*, 66(17), 814–821.

European Commission (2020). Communication from the Commission to the European Parliament and the Council of 13.11.2020. *New Consumer Agenda*, COM(2020) 696 final. https://eur-lex.europa.eu/legal-content/DE/ALL/?uri=COM:2020:696:FIN

Gielen, N., & Uphues, S. (2021). Digital Markets Act und Digital Services Act. *Europäische Zeitschrift für Wirtschaftsrecht,* 627–637.

Gigerenzer, G. (2008). *Gut feelings: The intelligence of the unconscious*. Penguin Books.

Gray, C. M., Kou, Y., Battles, B., Hoggatt, J., & Toombs, A. L. (2018). *The dark (patterns) side of UX design*. Conference Paper. Conference: CHI'18: Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems. At: Montréal, QU, Canada. Retrieved November 10, 2021, from https://www.researchgate.net/publication/322916969_The_Dark_Patterns_Side_of_UX_Design

Hausner, P., & Gertz, M. (2021). *Dark patterns in the interaction with cookie banners*. Preprint retrieved from https://arxiv.org/pdf/2103.14956.pdf

Kahneman, D. (2012). *Thinking, fast and slow*. Penguin Books.

Karpa, D., Klarl, T. & Rochlitz, M. (2022). Artificial intelligence, surveillance and big data. In Hornuf, L. (Ed.), *Diginomics Research Perspectives: The Role of Digitalization in Business and Society*, pp. @@@. Cham: Springer International Publishing.

Klein, K., Eisenbeiss, M., Dulle, M., Taherparvar, N., Wiemann, M. & Wiezorrek, J. (2022). Marketing in a digital world. In Hornuf, L. (Ed.), *Diginomics Research Perspectives: The Role of Digitalization in Business and Society*, pp. @@@. Cham: Springer International Publishing.

Kinra, A., Kotzab, H. & Siekmann, F. (2022). Social media analytics in operations and supply chain management: Opportunities, challenges and paradoxes. In Hornuf, L. (Ed.), Diginomics Research Perspectives: The Role of Digitalization in Business and Society, pp. @@@. Cham: Springer International Publishing.

Loy, C., & Baumgartner, U. (2021). Consent-Banner und Nudging. Tracking-Mechanismen: Wie viel „Anstupsen“ ist erlaubt? *Zeitschrift für Datenschutz*, 404–408.

Luca, M., & Bazerman, M. H. (2020). *The power of experiments: Decision making in a data-driven World*. MIT Press.

Luguri, J., & Strahilevitz, L. (2021). Shining a light on dark patterns. *Journal of Legal Analysis*, 13(1), 43–109. Retrieved November 10, 2021, from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3431205#

Martini, M., Drews, Ch., Seeliger, P., & Weinzierl, Q. (2021). Dark patterns. Phänomenologie und Antworten der Rechtsordnung. *Zeitschrift für Digitalisierung und Recht*, 47–74.

Mathur, A., Acar, G., Friedman, M. J., Lucherini, E., Mayer, J., Chetty, M., & Narayanan, A. (2019). Dark patterns at scale: Findings from a crawl of 11K shopping websites. Preprint retrieved from https://arxiv.org/pdf/1907.07032.pdf

Norwegian Consumer Council (2018). *Deceived by design*: *How tech companies use dark patterns to discourage us from exercising our rights to privacy*. Retrieved November 10, 2021, from https://fil.forbrukerradet.no/wp-content/uploads/2018/06/2018-06-27-deceived-by-design-final.pdf

Perlroth, N. (2021). *This is how they tell me the world ends: The cyberweapons arms race*. Bloomsbury Publishing.

Reisch, L. A. (2020). Nudging hell und dunkel: Regeln für digitales Nudging. Preprint retrieved from https://link.springer.com/content/pdf/10.1007/s10273-020-2573-y.pdf

Rieger, S., & Sinders, C. (2020). Dark patterns: Design mit gesellschaftlichen Nebenwirkungen. Retrieved November 10, 2021, from https://www.stiftung-nv.de/sites/default/files/dark.patterns.pdf

Sesing, A. (2021). Cookie-Banner – Hilfe, das Internet ist kaputt! *Multimedia und Recht*, 544–549.

Spindler, G., Thorun, Ch., & Blom, A. G. (2015). Die Evaluation der Button-Lösung. Ergebnisse einer empirischen Studie. *Multimedia und Recht (MMR)*, 3–7.

Sunstein, C. R. (2015). *Why nudge? The politics of libertarian paternalism*. Storrs Lectures on Jurisprudence.

Todd, P. M., & Gigerenzer, G. (2007). Environments that make us smart: Ecological rationality. *Current Directions in Psychological Science*, 16(3), 167–171. https://doi.org/10.1111/j.1467-8721.2007.00497.x

Utz, C., Degeling, M., Fahl, S., Schaub, F., & Holz. T. (2019). (Un)informed consent: Studying GDPR consent notices in the field. Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security, CCS 2019, London, UK, November 11–15, 2019. https://doi.org/10.1145/3319535.3354212

Weiss, A. (2013). Die Untiefen der "Button"-Lösung. *Juristische Schulung*, 590–594.

Weinzierl, Q. (2020). Dark Patterns als Herausforderung für das Recht. Rechtlicher Schutz vor der Ausnutzung von Verhaltensanomalien. *Neue Zeitschrift für Verwaltungsrecht* – Extra. 39. Jahrgang, Band 5, 1–11.