Legal Issues in the Digital Age. 2024. Vol. 5. No. 4.
Вопросы права в цифровую эпоху. 2024. Т. 5. № 4.

IT. Law. Human Rights

Research article
JEL*:* K00
УДК*:*34
DOI:10.17323/2713-2749.2024.4.4.27

Digital Abuse: How Dark Patterns Manipulate Our Lives

Boris Aleksandrovich Edidin[1]**,**
Ksenia Vladimirovna Kochetkova[2]**,**
Natalia Dmitrievna Sarankina[3]

[1, 2, 3] IRI, Institute for Digital Content Support & Development, 18 Tverskaya Street, Moscow 127006, Russia,

[1] b.edidin2018@gmail.com

[2] kochetkova.k@iri.center, Author ID: 1033155, ORCID ID: 0000-0002-6254-9539, Scopus ID: 57223024821

[3] sarankina.n@iri.center, Author ID: 1159548, Istina Researcher ID: 479507860

Abstract

The digital economy in Russia and abroad is of growing interest to lawmakers, especially in the context of the use of so-called 'dark patterns' — manipulative interface solutions that influence user behavior. BigTech companies consolidate their dominant position in the market by implementing innovative practices, many of which cannot be recognized as *bona fide*. The most prominent example of the implementation of user retention mechanisms through embedded features is the Tik Tok platform (Dou Yin). The Tik Tok phenomenon is still being studied by experts, but one of the clues is the unique recommendation feed that dynamically adjusts to the user's interests and is endless, creating the so-called "immersion effect". The article examines Russian and international approaches to regulating these practices. Particular attention is paid to legislative initiatives and enforcement practices aimed at protecting consumer rights and limiting the use of manipulative practices on digital platforms. The Russian legislation is still focused on certain aspects of consumer protection and countering unfair competition, while Western countries introduce specialized norms to combat “dark patterns”. The aim of the article is to examine the existing norms and suggest ways to adapt successful foreign practices to the Russian legal context.

Keywords

dark patterns; manipulative behavior; consumer data; GDPR; Digital Service Act, light patterns; unfair practices.

For citation: Edidin B.A., Kochetkova K.V., Sarankina N.D. (2024) Digital Abuse: How Dark Patterns Manipulate Our Lives. *Legal Issues in the Digital Age*, vol. 5, no. 4, pp. 4–27. DOI:10.17323/2713-2749.2024.4.4.27

Introduction

Big Tech companies, especially the owners of social networks, are among the key actors of the data economy that operates “big data”. In the doctrine “big data” is described as large amounts of diverse information with high speed of formation and fast processing [Blazheev V.V., Egorova M.A., 2021: 121]. As noted by foreign specialist, human (consumer) data is becoming the most important natural resource in the era of AI [Webb E., 2022: 5] Artificial intelligence collects, processes and analyzes data automatically, which allows data operators to accumulate a huge amount of information about individuals.

Any data about human life is commercialized, not only in the form of a separate set of initial information (known as raw data), but also in the form of pre-processed information. Many different data exchanges operate all over the world. These are real B2B marketplaces that sell sets of user data (e.g., Oracle Data Marketplace, Think Data Works Marketplace).

In the doctrine this trend has been called the phenomenon of “surveillance capitalism” — a new stage in the development of the digital age, which is characterized by the total surveillance of the user by technology giants Digital companies are able not only to monitor the user, but also to influence their behavior [Zuboff S., 2022: 157, 251].

Massive, automated analysis allows online companies to perform profiling. In the digital technologies sphere profiling refers to any form of automated processing of personal and other data about an individual to assess, analyze, or predict any personal features like economic status, health, preferences and interests, location, or possible behavior of an identifiable person. During such profiling, the user receives pre-filtered information, thus transforming his or her behavior.

Specific manipulation techniques can be used in the digital environment. It has become possible to induce consumers to purchase a product or service by manipulating the appearance of a mobile application, Internet page or other digital service.

Such tricks in the design of the user interface are called “dark patterns”. Why dark? Because these methods are unfair and undesirable for the consumer, but profitable for the company. Thus, they lead to so-called “digital market manipulation” [Calo R., 2014: 995].

Since the concept of “dark patterns” entered the legal field recently, its analysis has a high scientific theoretical and practical value.

The article provides a thorough legal analysis of manipulating consumer behavior on the Internet. The authors are briefly explaining the phenomenon of consumer behavior manipulation; explain what the “dark patterns” are in its nature; present comparative legal analysis of approaches to the regulation of “dark patterns”, including Russian stance on manipulative design and provide relevant case study.

1. Interpretation of the Term “Dark Patterns”

The term was introduced in 2010 by Harry Brignall, a specialist in user interface, and refers to “design methods that deceive or manipulate users into making choices they would not otherwise make and that can cause harm”.[1]

In other words, “dark patterns” are unscrupulous tricks when designing the appearance of a website, mobile app, or other digital service.

In the practice of user-centered design, “UX laws” are beginning to emerge that vividly illustrate methods of visual manipulation [Yablonski D., 2022: 2]. For example, tricks may concern the location of links (“law of similarity”), highlighting this or that choice with a certain color (“isolation effect”, or “von Restorff effect”).

“Dark patterns” can be classified into three types depending on what effect they are aimed at achieving:

[1] Available at: https://alistapart.com/article/dark-patterns-deception-vs.-honesty-in-ui-design/ (accessed: 05.09.2024)

obtaining a direct commercial benefit for the entrepreneur (e.g., inducing the user to purchase a product or service);

obtaining an indirect commercial benefit (e.g., forcing the user to view an advertisement);

increasing the user's interest in the platform (e.g., forcing the user to stay on the platform as long as possible).

Interestingly, some analytics distinguish among visible dark patterns (mentioned ones), darker patterns (less detectable dark patterns such as "forced practices" and "fragmented data protection information") and the darkest patterns (detective design techniques purposely integrated into an online service's system architecture (SA) or code level and not on the UI/UX). [Leiser M.R., Santos C., 2024: 5, 10, 18].

It is useful to illustrate "classic dark patterns" with an example.

When inclining the consumer to purchase a product or service, the owner of the platform receives a direct and specific commercial benefit. Thus, by offering the user several options for a paid subscription to the service (for example, for 1 month, 6 months and 1 year) and highlighting the option with a longer term and higher price, but with a discount relative to this price, the user is visually "hinted" at the profitability of this option compared to the option with a shorter term and low price [Duplyakin W.M., Knjazheva V.V., 2016: 36].

When a consumer is forced to view an advertisement, the entrepreneur receives an indirect benefit, as he receives a monetary reward for the from the advertiser.

In addition, sometimes in advertisements the button to close the advertisement is "masked" to make it harder for the user to find.

Compulsion to stay on the platform as long as possible is used in one way or another by all major platforms, especially social networks. These methods include endless scrolling, checking likes/dislikes. Such mechanisms are always destructive for the user, as they can cause Internet addiction.

Currently, game addiction is included in the International Classification of Diseases (ICD-11) of the World Health Organization.[2] However, Internet addiction is absent in ICD-11. It's most likely due to insufficient study of the real impact of the Internet on human physical and mental health. At

[2] Available at: https://icd.who.int/browse/2024-01/mms/en#338347362 (accessed: 05.09.2024)

the same time, game addiction was included in the ICD relatively recently, in 2022, so, in our opinion, the global medical community will continue to work on studying the destructive impact of other forms of digital interaction. It is necessary to study those mechanics of digital platforms, especially social networks, that cause real addictive behavior.

Thus, the design of a digital service's appearance can indeed mislead, induce action, or otherwise manipulate an individual's behavior. The harmfulness of these practices may be magnified for less protected populations, which include minors or the elderly. Some specialists believe that "contractual consent secured via pernicious forms of dark patterns or other deceptive designs should be deemed invalid as a matter of law" [Hartzog W., 2018: 212–213].

Unsurprisingly, the following harms have been associated with the use of dark patterns: 1) lower autonomy; 2) a reduction in overall social and consumer welfare; 3) an erosion of trust; 4) increased insecurity; and 5) unfair treatment among consumers. [Leiser M.R., Caruana M., 2021: 242].

This unscrupulous behavior cannot go unnoticed by regulators, so foreign legal orders are gradually developing competent positions on the use of "dark patterns".

2. Manipulation of Consumer Behavior on the Internet: Regulative Approach

2.1. Regulation of "Dark Patterns" in the USA

In October 2021 the U.S. Federal Trade Commission (hereinafter FTC) has issued an enforcement policy statement warning companies against using illegal practices such as automatic renewal of paid subscriptions, free trial periods of subscriptions with automatic paid renewals, and few other manipulations.[3]

Previously, in April of the same year, the FTC held a public workshop on the topic of dark patterns in the digital environment, which resulted in the release of the Federal Trade Commission Report on Dark Patterns.[4]

[3] Enforcement Police Statement Regarding Negative Option Marketing // Federal Trade Commission. 2021. Available at: https://www.ftc.gov/system/files/documents/public_statements/1598063/negative_option_policy_statement-10-22-2021-tobureau.pdf (accessed: 05.09.2024)

[4] FTC Report Shows Rise in Sophisticated Dark Patterns Designed to Trick and Trap Consumers. 2022. Available at: https://www.ftc.gov/news-events/

The report does not develop its own definition of "dark patterns" but uses the classic definition by Harry Brignall.

The FTC report identifies types of dark patterns such as creating false beliefs (e.g., advertisements designed as news articles), concealing or delaying disclosure of material information (e.g., concealing a fee charge or including it in the price only at the end of a purchase), pushing consumers to make payments (e.g., offering a free trial of a product with automatic renewal of recurring payments), and violating privacy (e.g., failing to provide sufficient privacy settings).

The document also states that the FTC on will act against companies' use of those techniques that would directly violate U.S. law or other regulations enforced by the regulator. Such acts include, for example, The Restore Online Shoppers' Confidence Act (ROSCA)[5], The Telemarketing Sales Rules (TSR)[6], The Truth in Lending Act (TILA), The Children's Online Privacy Protection Act (COPPA)[7].

A month later the same year, the Deceptive Experiences to Online Users Reduction Act (DETOUR)[8] was introduced in the U.S. Senate. The initiative aims to completely ban exploitative and misleading practices by major online platforms and improve consumer welfare. The draft rules do not call directly "dark patterns", but uses the term "unfair and misleading practices related to the manipulation of the user interface".

The varieties of such practices are separately identified as:

designing, altering, or manipulating the user interface to conceal, undermine, or infringe on user autonomy, to influence decision-making, or to provide user data;

news/press-releases/2022/09/ftc-report-shows-rise-sophisticated-dark-patterns-designed-trick-trap-consumers (accessed: 05.09.2024)

[5] Restore Online Shoppers' Confidence Act of 2010. Available at: https://www.ftc.gov/legal-library/browse/statutes/restore-online-shoppers-confidence-act (accessed: 05.09.2024)

[6] Telemarketing Sales Rules of 2022. Available at: https://www.ftc.gov/legal-library/browse/rules/telemarketing-sales-rule (accessed: 05.09.2024)

[7] Children's Online Privacy Protection Rule of 1998. Available at: https://www.ftc.gov/legal-library/browse/rules/childrens-online-privacy-protection-rule-coppa (accessed: 05.09.2024)

ф[8] Deceptive Experiences to Online Users Reduction Act. H.R.6083 of 2021. Available at: https://www.congress.gov/bill/117th-congress/house-bill/6083?s=1&r=30 (accessed: 05.09.2024) subdividing or segmenting consumers of online services into groups for the purpose of behavioral or psychological experimentation or research on users of an online service, except with the informed consent of each user involved; or

designing, modifying, or manipulating the user interface on a website or online service intended for persons under the age of 13 to encourage habituation to the service.

After the bill was sent to the Consumer Protection and Commerce subcommittee in December 2021, there was no further movement on this legislative initiative.

In January 2023 the Future of Privacy Forum (hereinafter FPF) has published the current position of U.S. regulators on dark patterns.[9] In particular, it highlighted key trends explaining the most significant rules that address manipulative design in the US data protection context and highlighted the opportunities and challenges of applying anti-manipulative design rules to specific business sectors or practices. It was noted that most state laws aimed at limiting or prohibiting the use of manipulative design are based in one way or another on the already mentioned DETOUR bill.

Indeed, several laws have been drafted and passed at the state level that focus on banning "dark patterns."

The first state-level act regulating dark patterns was the California Consumer Privacy Act (CCPA)[10], now amended and supplemented by the California Privacy Rights Act (CPRA).[11] It was the first legislation in the USA to explicitly regulate dark patterns. The current document defines a "dark pattern" as "a user interface designed or operated with the substantial effect of undermining or limiting a user's autonomy in making decisions or exercising choices." If a company fails to comply with the requirements of this law, the state attorney general may file a lawsuit that will result in the offending company being fined. The amount of the fine is determined by the applicable unfair competition law. Interestingly, the CPRA includes a

[9] Slater F. The Future of Manipulative Design Regulation // Future of Privacy Forum. 2023. Available at: https://fpf.org/blog/the-future-of-manipulative-design-regulation/ (accessed: 10.09.2024)

[10] California Consumer Privacy Act of 2018 (CCPA) // Available at: https://oag.ca.gov/privacy/ccpa (accessed: 10.09.2024)

[11] California Privacy Rights Act of 2020 (CPRA) // Available at: https://www.oag.ca.gov/sites/all/files/agweb/pdfs/privacy/oal-sub-final-text-of-regs.pdf (accessed: 10.09.2024)

provision that explicitly forbids obtaining consent related to the processing of personal information by means of dark patterns [King J., Stephan A., 2021: 267].

Speaking about the requirements to the interface design, it should be noted that the concept of age-appropriate design (age-appropriate design) is also gaining popularity. In the US, this concept is regulated by the California state law (the California Age-Appropriate Design Code Act–CA AADC)[12], the Illinois legislative initiative (SB 3334)[13] and the federal bill on the safety of children on the Internet (Kids Online Safety Act — KOSA)[14].

Under this framework, website and mobile app owners are encouraged to check the appearance of online pages, algorithms, and service targeting ads for the "dark patterns" that entice children to provide excessive data, remove privacy settings, or otherwise act against children's interests.

Hence, in many ways, age-appropriate design and "dark pattern-free" design are two elements of the same idea, which boils down to developing certain requirements for the interface of mobile apps and websites.

Thus, there is a trend in the U.S. to adopt special norms aimed at regulating "dark patterns" as special unfair and misleading practices related to the manipulation of the user interface. In addition, actual jurisprudence is also gradually emerging from the norms being approved.

2.2. Regulation of "Dark Patterns" in the EU

The General Data Protection Regulation (GDPR) does not set out a definition of dark patterns, but several its provisions somehow indicate a prohibition of unfair practices against consumers.[15] These provisions include: the principle of fairness and transparency (Article 5(1) (a), the principle of accountability in Article 5(2), data protection by default (Article 25), the requirement to provide data subjects with transparent privacy

[12] Available at: https://leginfo.legislature.ca.gov/faces/billCompareClient.xhtml?bill_id=202120220AB2273&showamends=false (accessed: 10.09.2024)

[13] Available at: https://www.ilga.gov/legislation/fulltext.asp?DocName=&SessionId=112&GA=103&DocTypeId=SB&DocNum=3334&GAID=17&LegID=&SpecSess=&Session= (accessed: 10.09.2024).

[14] Available at: https://www.congress.gov/bill/118th-congress/senate-bill/1409/text (accessed: 10.09.2024)

[15] Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679 (accessed: 10.09.2024)

notices (Article 12(1), 13 and 14), and other rights of personal data subjects under the GDPR in Articles 15-22.

The European Digital Services Act (DSA) that has came into force in August 2023, explicitly prohibits the use of "dark patterns" in the online interfaces of digital platforms.[16] The law defines "dark patterns" as "practices that materially distort or impair, either on purpose or in effect, the ability of recipients of the service to make autonomous and informed choices or decisions".

Actual enforcement practices are also beginning to emerge as part of the implementation of this law. For example, in December 2023 the European Commission has launched an investigation into the social network X (ex-Twitter) for "dark patterns" prohibited by the DSA on its services.[17]

In 2023 the European Commission and the national consumer protection authorities of 23 EU states, as well as the consumer protection authorities of Norway and Iceland, published the results of an audit of retail websites covering 399 online stores.[18]

The study focused manipulative practices on the sites, which included fake countdown timers, web interfaces designed to induce consumers to make purchases, subscriptions or other choices, and hidden information.

According to the study, 148 websites contained at least one "dark pattern." 42 websites used fake countdown timers with deadlines to purchase certain products; 54 websites steered consumers toward certain choices, from subscriptions to more expensive products or delivery options; and 70 websites hid important information or made it less visible to consumers. For example, information about delivery costs, product composition or the availability of a cheaper option.

Several acts were approved as a result of the pan-European audit.

For example, in December 2023 the European Parliament has passed a resolution on addictive digital service design.[19] In particular, the Parliament

[16] Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022R2065&qid=1666857835014 (accessed: 10.09.2024)

[17] Available at: https://ec.europa.eu/commission/presscorner/detail/en/IP_23_6709 (accessed: 10.09.2024)

[18] Available at: https://ec.europa.eu/commission/presscorner/detail/en/ip_23_418 (accessed: 10.09.2024)

[19] Available at: https://www.europarl.europa.eu/doceo/document/TA-9-2023-0459_EN.pdf (accessed: 10.09.2024)

advocated the introduction of rules restricting the use of "dark patterns" by platforms that are addictive to consumers. The introduction of such rules seems relevant, as many platforms are now equipped with mechanics of involving the user in "endless" consumption of digital content, that can significantly harm his physical and mental health.

Also in December 2023, the Regulation on Harmonized Rules for Fair Access to and Use of Data (Data Act) was approved.[20] The Act prohibits the use of "dark patterns" by personal data operators or third parties to whom personal data is transferred with the consent of the user. This provision meets the principle of data minimization enshrined in the GDPR, aimed at prohibiting the collection of so-called excessive data, and allows to give additional legal guarantees to the user when transferring his data to third parties.

One of the objectives of the Directive on Financial Services Contracts Concluded at a Distance is to prevent traders, when concluding financial services contracts at a distance, from using dark patterns in their online interfaces [Brenncke M., 2023: 49].

Separately, attention should be paid to "dark patterns" in social networks.

In March 2022, the European Data Protection Board (EDPB) has published draft Guidelines 3/2022 "Dark patterns in social media platform interfaces: how to recognize and avoid".[21] This document has become a practical guide for both developers and users of social media platforms. It defines "dark patterns" as "interfaces and user experiences implemented on social media platforms that lead users into making unintended, unwilling, and potentially harmful decisions regarding the processing of their personal data."

The use of each dark patterns model is detailed according to the specific life cycle of a social media account: opening a social media account; informing on social media; protecting on social media; exercising personal data rights on social media; and deleting a social media account.

The draft recommendation for social media identifies types of "dark patterns" such as:

[20] Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32023R2854 (accessed: 10.02.2024)

[21] Available at: https://edpb.europa.eu/system/files/2022-03/edpb_03-2022_guidelines_on_dark_patterns_in_social_media_platform_interfaces_en.pdf (accessed: 10.09.2024)

“overloading” — overloading users with more requests, information or options to encourage them to provide more data;

“skipping” — designing the interface in such a way that users forget (or fail to consider) all or some aspects of data protection when making a decision;

“stirring” — appealing to users’ emotions or using visual tricks;

“hindering” — hindering in obtaining information about the use of data or exercising control over data;

“fickle” — designing an awkward interface that makes it difficult to navigate or understand the purpose of data processing;

“left in the dark” — designing the interface in such a way as to hide information.

A lot of measures are also being taken in EU countries.

For example, in 2019 French data authority has released the report that defined “dark patterns” as “elements and mechanisms of interfaces implemented to influence users’ decisions in a way that they would not necessarily choose if the information was presented honestly and transparently”.[22]

In Belgium in October 2023 a checklist on the use of cookies was published. One of the items on the checklist is the absence of the use of “dark patterns” in the consent to accept cookies.[23]

The Luxembourg National Commission for Data Protection published updated recommendations on the use of cookies, according to which “dark patterns” include various shapes, fonts, colors, and sizes of “I accept” and “I decline” buttons.[24]

In Germany, based on the Research Institute for Public Administration (Deutsches Forschungsinstitut für öffentliche Verwaltung) within the framework of the Dark Pattern Detection Project (Dapde) there is an interdisciplinary group of scientists in the field of information technology and legal studies engaged in the search on technical detection of “dark patterns”

[22] Available at: https://linc.cnil.fr/cahier-ip6-la-forme-des-choix (accessed: 10.09.2024)

[23] Available at: https://www.autoriteprotectiondonnees.be/citoyen/actualites/2023/10/20/lapd-publie-une-checklist-pour-une-utilisation-correcte-des-cookies accessed: 10.09.2024)

[24] Available at: https://fil.forbrukerradet.no/wp-content/uploads/2018/06/2018-06-27-deceived-by-design-final.pdf (accessed: 13.09.2024)

and preparation of the necessary regulatory framework for their regulation.[25] Researchers use the now classic definition of "dark patterns" given by Harry Brignall.

The main tools of protection against "dark patterns", as follows from the information about the project, should be considered the norms of legislation on data protection, consumer protection, and competition protection.

Thus, approaches to the regulation of dark patterns are also beginning to take shape in EU countries. Approaches are being formed both at the supranational level, i.e. at the level of the European Union, and at the national level, i.e. at the level of individual EU states. At the same time, the regulatory approaches of the EU countries obviously follow in line with common European practices, as evidenced by similar terminology and similar rules for combating "manipulative design".

2.3. Regulation of "Dark Patterns" in the UK

In January 2021 the UK Competition and Markets Authority (CMA) has published a paper "Algorithms: How They Can Reduce Competition and Harm Consumers", which identified the need for joint regulation of dark practices with the UK Information Commissioner.[26] It defined "dark patterns" as "user interface designs that are used in such a way as to trick users into making unintended or potentially harmful decisions".

Two years later, in August 2023 the Competition and Markets Authority (CMA) and the Information Commissioner's Office (ICO) have published a joint paper "Harmful design in digital markets: how online choice architecture practices can undermine consumer choice and control over personal information" aimed at web designers and developers and outlines a set of best practices for providing consumers with information and choice about the collection and use of their personal information.[27]

The guidance lists "dark patterns" (e.g., "harmful nudging," "guilt-tripping," "batch consent," and "default settings") and highlights a few risks

[25] Available at: https://dapde.de/de/ (accessed: 13.09.2024)

[26] Available at: https://www.gov.uk/government/publications/algorithms-how-they-can-reduce-competition-and-harm-consumers/algorithms-how-they-can-reduce-competition-and-harm-consumers (accessed: 13.09.2024)

[27] Available at: https://www.drcf.org.uk/__data/assets/pdf_file/0024/266226/Harmful-Design-in-Digital-Markets-ICO-CMA-joint-position-paper.pdf (accessed: 13.09.2024)

associated with companies' use of dark patterns. Among other things, the authors of the guide supplement each "pattern" with a specific example illustrating a negative practice.

In 2020 an age-appropriate design code of practice, the so-called Children's Code, has came into force in the UK.[28] The document, which predates the California law and other U.S. initiatives, calls for basic "default" settings to be provided in a way that ensures children's safe access to online services and minimizes the collection and further use of children's data.

2.4. Regulation of "Dark Patterns" in Other Jurisdictions

In 2023 the Central Consumer Protection Authority of India has published Guidelines for Prevention and Regulation of Dark Patterns.[29] The document defines "dark patterns" as any practice or deceptive design pattern using user interface or user interaction on any platform that is intended to mislead or deceive users into doing something they did not originally intend or want to do, by undermining or impairing consumer autonomy, decision-making or choice, amounting to misleading advertising or unfair trade practices or consumer infringement. It provides a list of prohibited dark patterns with examples explaining them. However, these Guidelines are non-binding and lawyers are questioning their effectiveness due to lack of enforcement.

The Korea Republic Government is currently advocating for an amendment to the Act on The Consumer Protection in Electronic Commerce. The amendments would address "dark patterns", which have been declared an important consumer policy issue by the Commission and are supposed to develop means to prevent online platforms from deceiving users.[30]

In January 2022 the Information and Communication Technology Task Force was transformed into The Digital Markets Response Team. The Digital Consumer Division within it monitors and eliminates new behaviors designed to deceive consumers (including the use of "dark patterns"), en-

[28] Available at: https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/childrens-information/childrens-code-guidance-and-resources/age-appropriate-design-a-code-of-practice-for-online-services/code-standards/ (accessed: 13.09.2024)

[29] Available at: https://consumeraffairs.nic.in/theconsumerprotection/guidelines-prevention-and-regulation-dark-patterns-2023 (accessed: 13.09.2024)

[30] Available at: https://www.kimchang.com/en/insights/detail.kc?sch_section= 4&idx=22891 (accessed: 13.09.2024)

sures that consumer choice is available and that consumers have sufficient information to make informed decisions.[31]

In June 2022 the UK and Singapore have signed the UK-Singapore Digital Economy Agreement (DEA).[32] According thereto both states are committed to ensuring fair online trading and protecting consumers from fraudulent or unfair business practices (including "dark patterns").

In July 2023 Kazakhstan has approved the law "On Online Platforms and Online Advertising".[33] The new legislation has a broad subject of regulation — from the legal regime of operation of online platforms and online advertising to the legal status of influencers (bloggers). At the same time, as far as online platforms are concerned, the law states that their interface should not mislead or otherwise prevent the user from deciding.

3. Case Study

In the absence of strict and clear rules applicable to dark patterns, it is possible only to witness some activity on this issue from the judiciary and other authorities. Because these tricks were used by business to attract more users and thus gain more profit, there are various lawsuits against big companies alleging consumer manipulation.

The European Union has already developed its law enforcement practice (on every state level). For example, the Italian data protection authority (Garante) has fined a company providing digital marketing services 300 thousand euros for illegal processing of personal data using "dark patterns".[34] According to Garante, through various manipulative techniques, the digital platform induced users to consent to the processing or to the transfer of their data to third parties.

The U.S. Federal Trade Commission has recently intensified its actions in the fight against dark patterns.

[31] Available at: https://www.kimchang.com/en/insights/detail.kc?sch_section=4&idx=24536 (accessed: 13.09.2024)

[32] Available at: https://www.gov.uk/government/publications/uk-singapore-digital-economy-agreement-explainer/uk-singapore-digital-economy-agreement-final-agreement-explainer (accessed: 13.09.2024)

[33] Law of the Republic of Kazakhstan of July 10, 2023 №18-VIII ZRC On online platforms and online advertising // Egemen Kazakhstan. 2023. № 128 (30607).

[34] Available at: https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9870725#1 (accessed: 13.09.2024)

In 2023 the Commission has reached a 18,5 million dollars settlement with Publishers Clearing House for engaging in misrepresentation and deceptive practices.[35] According to the FTC, the PCH Publishers Clearing House employed various manipulative practices, e.g. the use of extra-small and too-light fonts for disclosure notices and links and adding shipping and handling fees late in the checkout process.

One of the biggest-scale cases on that matter concerns Amazon. According to the lawsuit, "Amazon has knowingly duped millions of consumers into unknowingly enrolling in Amazon Prime and used manipulative, coercive, or deceptive user-interface designs known as "dark patterns" to trick consumers into enrolling in automatically renewing Prime subscriptions".[36] On 28 May 2024, a federal judge has handed down a decision allowing the lawsuit to proceed. Furthermore, the Judge has ruled that the Commission's claim was sufficiently plausible, indicating that a reasonable consumer who clicks on the orange "Get FREE Two-Day Delivery" button may not be aware that they are consenting to the automatic renewal of a Prime subscription. Additionally, the visual discrepancy between the "yes" and "no" buttons may lead consumers to believe that clicking "yes" is the only option for completing the checkout process. Moreover, the Judge Chun has expressed concern that Amazon made it considerably more difficult to cancel a Prime subscription than to enroll in Prime.

The most recent case to-date is a lawsuit brought against Adobe by the FTC and the Department of Justice in June 2024.[37] Adobe and two of its executives are charged with deceiving consumers by concealing the early termination fee for its most popular subscription plan and making it challenging for consumers to cancel their subscriptions.

Similar accusations were thrown at Google in 2022.[38] Then the Attorney General for the District of Columbia has filed a lawsuit a complaint to stop Google's violations of the District's consumer protection laws, which included the use of dark patterns to undermine users' informed choices (for

[35] Available at: https://www.ftc.gov/system/files/ftc_gov/pdf/PCH-Complaint.pdf (accessed: 13.09.2024)

[36] Available at: https://www.ftc.gov/system/files/ftc_gov/pdf/amazon-rosca-public-redacted-complaint-to_be_filed.pdf (accessed: 13.09.2024)

[37] Available at: https://www.ftc.gov/system/files/ftc_gov/pdf/040-UnredactedComplaint.pdf (accessed: 13.09.2024)

[38] Available at: https://oag.dc.gov/sites/default/files/2022-01/DCv.Google%281-24-22%29.pdf (accessed: 13.09.2024)

instance, the could not easily opt out of having their location tracked). The very same year Google has decided to settle the lawsuit.[39] According to the settlement, Google had to pay 9,5 million dollars fine to the District as well as issue notifications to users who currently have certain location settings enabled; clearly inform users about data collection when they enable location-related Google account settings; maintain a webpage that discloses Google's policies and practices concerning location data; improve users' ability to identify location-related controls; limit sharing of users' data and retention of data; prepare annual compliance reports.

These three are the most recent FTC cases involving Big Tech companies. However, before that it has already tried to fight various dodgy tactics taken by companies to lure customers (e.g. Federal Trade Commission v. AMG Capital Management; Federal Trade Commission v. Office Depot). In a series of unheralded FTC deception cases, and in a few unfairness enforcement actions to boot, the regulator best positioned to address dark patterns has successfully shut down some of the most egregious ones [Luguri J., Strahilevitz J.A., 2021: 102]. In the overwhelming majority of enforcement actions, companies choose to settle with the Commission entering into binding settlement agreements, but not to challenge the commission in court or administrative proceedings [Solove D.J., Hartzog W., 2014: 583].

Also worth noting is that just until recently (recently being the cases against Adobe, Google and Amazon) courts, despite substantive scholarship on dark patterns, in the United States and the FTC have not been proactively using the term "dark patterns" when issuing decisions policing manipulative user interfaces [Nousiainen C.P., Ortega K., 2024: 92].

It can also be said that the lack of direct regulation of dark patterns does not automatically mean that it is impossible to sue companies for using a manipulative interface. Before Indian Guidelines of 2023 were passed, in 2021 the Hyderabad District Disputes Redressal Commission has fined online ticket aggregator Book My Show and PVR cinemas for imposition of Internet handling charges on the customers. The Commission's order has indicated that the imposition of internet handling charges in the final bill amount without a clear segregation is equal to an unfair trade practice, thus it violates the Consumer Protection Act of 2019. Basically, the Commission has qualified the imposition of Internet handling charges in the

[39] Available at: https://oag.dc.gov/release/ag-racine-announces-google-must-pay-95-million (accessed: 13.09.2024)

final bill amount as hidden cost practice (one of the types of dark patterns) [Sharma S.J., Sharma I., 2023: 143].

4. Russian Approach

Digital economy in Russia is regulated both through the new legislative norms and self-regulation, e.g. the codes of conduct, guidelines, recommendations, and sets of best practices.

The main laws that set up an official framework for digital technologies in Russia are the Civil Code of the Russian Federation[40], the Federal Law "On Personal data"[41], the Federal Law "On Information, Information Technologies and Protection of Information".[42]

Article 10.6 of the Federal Law "On Information, Information Technologies and Information Protection" sets up a number of obligations for social networks owners. For intense, they are obligated to monitor and remove prohibited information, to create a feedback tool for users' appeals, and to annually publish a report on the results of such "self-control".

That is, these norms are designed to ensure self-regulation of social networks, which were originally created on the basis of such self-regulation.

No less important, but less frequently mentioned in the context of the digital economy is the Law of the Russian Federation on Protection of Consumer Rights.[43] Particularly, this legal act regulates the consumer purchase of goods or services on the Internet.

Article 10 of the Law "On Protection of Consumer Rights" enshrines the obligation of the producer or seller to provide the consumer with necessary and reliable information about goods, works or services, ensuring the possibility of their correct choice. However, the Russian law does not contain any provisions prohibiting the using of the "dark patterns".

[40] Civil Code of the Russian Federation // Collected Laws of Russia. 1994. No.32. Article 3301.

[41] Federal Law of the Russian Federation of July 27, 2006 No.152-FZ On Personal Data // Rossiyskaia Gazeta, 2006, № 165.

[42] Federal Law of the Russian Federation of July 27, 2006 No.149-FZ On Information, Information Technologies and Information Protection // Ibid.

[43] Law of the Russian Federation of February 7, 1992 No. 2300-I On Protection of Consumer Rights // Bulletin of the Congress of People's Deputies of the Russian Federation and Supreme Council of the Russian Federation. 9.04.1992. № 15. Art. 766.

Speaking about misrepresentation in general, it is worth to mention the Federal Law "On Protection of Competition".[44] In particular, Article 14.2 of this law prohibits unfair competition by misrepresentation.

The responsibility for unfair competition by misrepresentation is laid down by the Article 14.33 of the Code of Administrative Violations.[45] At the same time, Article 14.7 of the Code establishes liability for consumer deception and misleading consumers. Article 14.8 of the Code provides for administrative responsibility for violation of the consumer's right to receive necessary and reliable information.

Thus, liability for misleading for the purposes of unfair competition differs from misleading the consumer without violation of law. It should be noted that the legal relations between business and the consumer and their ethical component, i.e. the interaction of subjects in the B2C segment, is the main idea of the article.

As it was already mentioned, "dark patterns" as methods of manipulating of user behavior are closely connected with the creating of visual effects. Moreover, their use is not always aimed at obtaining a direct commercial benefit in the form of payment of consumers for a certain product or service.

Sometimes "dark patterns" may fall, for example, under the law on advertising.

Thus, according to the Part 7 of Article 5 of the Federal Law "On Advertising" it's prohibited to make advertisements, which do not contain part of the essential information about the product, the conditions of its purchase or use, if it distorts the meaning of information and misleads the consumer.[46]

Part 9 of Article 5 prohibits hidden advertising, that has an unconscious impact on the consumers.

As it was correctly noted by the press service of the Federal Antimonopoly Service of Russia, the dissemination of incomplete information or concealment of its significant part are the main ways of misleading.[47]

[44] Federal Law of July 26, 2006 № 135-FZ On Protection of Competition // Rossiyskaia Gazeta. 2006. №162.

[45] Code of the Russian Federation on Administrative Violations of December 30, 2001 № 195-FZ // Rossiyskaia Gazeta. 2001. № 256.

[46] Federal Law of March 13, 2006 No. 38-FZ On Advertising // Parliamentskaia gazeta. 2006. №37.

[47] Available at: URL: https://fas.gov.ru/publications/20367?ysclid=ltya9u3ner23880392 (accessed: 10.10.2024)

Authors of the article would like to emphasize the recent changes in the legislation on advertising, expressed in the adoption of new requirements for advertising of credit products.[48]

In 2023 the requirements to the print in the advertisements of credit products came into force. According to the amendments, the size of the print used to indicate the ranges of values of the full value of the consumer loan should not be smaller than the size of the font used to indicate information on interest (percentage) rates.

In October 2023 the credit organization "Pochta Bank" was fined for failure to comply with the FAS order to remove this kind of improper advertising.[49] In February 2024, cases were brought against Alfa Bank and Sberbank on the same ground.[50] [51]

All in all, some aspects of the "dark patterns" — for example, the possibility of misleading through manipulation of prints — could be found in the specific legislation and law enforcement practice.

At the same time neither general regulation of the manipulative interface design practices nor special terminology is introduced.

Nevertheless, the competent authorities are gradually beginning to form their positions.

In November 2023 the Bank of Russia has issued a report "Approaches to the Regulation of Remote Sales Channels to Protect the Rights of Financial Services Consumers".[52] In the report, the Bank highlighted such unfair practices in the online sale of financial products as the use of ambiguous or difficult-to-understand wording, graphic and color techniques that focus the consumer's attention on certain terms of the contract or additional services.

The Bank of Russia has defined "dark patterns" as "various marketing techniques that encourage consumers to take certain actions".

[48] Federal Law № 359-FZ of July 24, 2023 "On Amendments to the Federal Law On Consumer Credit (Loan)' and certain legislative acts of the Russian Federation // Rossiiskaia Gazeta.2023. №168.

[49] Available at: URL: https://fas.gov.ru/news/32852 (accessed: 10.10.2024)

[50] Available at: URL: https://fas.gov.ru/publications/24254 (accessed: 10.10.2024).

[51] Available at: URL: https://fas.gov.ru/publications/24273 (accessed: 10.10.2024)

[52] Available at: URL: https://cbr.ru/Content/Document/File/156122/Consultation_Paper_13112023.pdf (accessed: 10.10.2024)

Basing on the results of the report, the Bank offers a number of proposals to regulate the practice of selling financial products. For instance, one of the proposals is to completely eliminate the use of "dark patterns" in the banking.

In June 2022 the Regional Public Center of the Internet Technology (ROCIT) has presented an analytical report on manipulation of user behavior using "dark patterns".[53]

ROCIT experts has defined "dark patterns" as "techniques of manipulating user behavior with the help of the device and design of a website, application or digital services, aimed at inducing the user to make decisions that are beneficial for a commercial company".

The authors of the study identified such types of dark patterns as:

coercion — threatening or requiring the user to fulfill certain requirements (requiring the user to enter contact information before allowing the user to complete a task);

confusing — asking information from the user that they do not understand (asking a novice user if they want to change the default browser; using double, triple or quadruple negation);

distraction — distracting the user from their actual task in order to redirect their attention to areas of the interface that are beneficial to the company (a red button on the desired interface element to draw attention);

utilizing user errors in order to achieve the actions desired by the interface designer;

compulsory work — deliberately increasing the amount of work for the user (making the user wait and view an advertisement for a certain amount of time);

interruption — interrupting the flow of a user's tasks;

canipulation of navigation: creating information architectures and navigation mechanisms that direct the user to perform a desired action (a free version of an application is much harder to find than a commercial version);

concealment — hiding necessary information and interface elements;

restriction of functionality — limiting or excluding controls that facilitate the user's task;

[53] Available at: URL: https://t.me/IT_today_ru/5776 (accessed: 10.10.2024)

shock — presenting disturbing content to the user;

subterfuge — misleading the user or other attempts to deceive (installation of additional software without the user's knowledge or consent).

In order to combat such unfair practices, ROCIT experts propose the development of uniform rules, regulation by the state and public organizations, and the introduction of negotiable fines for repeated violations.

As was mentioned above, "dark patterns" may also be manifested through the functioning of recommendation technologies.

In the fall of 2023 the Alliance for Artificial Intelligence has developed guidelines for the use of recommendation technologies and algorithms based on artificial intelligence.[54] The document contains several principles for the ethical use of recommender algorithms, some of which can also be used in the prevention of the use of "dark patterns".

For example, the experts draw attention to recommendations that turn into imposition and note that their use is not advised.

Also, the authors of the document emphasize the need to combat the manipulation of algorithms, through which you can influence the user's perception of a particular product, the feasibility of its purchase, to "tweak" the popularity of a particular content.

Among other things, experts of the Alliance in the field of artificial intelligence advise to implement recommendations that suggest the user to take certain actions to preserve health, including interrupting the use of the service for rest or sleep. This practice seems relevant in the fight against digital services based on "pulling" the user into a long-term session, for example, through the system of endless scrolling of the feed. This was already mentioned in the first chapter of the study, when the "TikTok phenomenon" was considered.

Thus, at present in Russia there is no special normative regulation or advisory acts devoted to the prohibition of "dark patterns" and other ways of manipulating consumer behavior on the Internet.

In one way or another there may be norms in the legislation that can be applied to "dark patterns", however, they will affect only one narrow aspect of such unfair practices (for example, "dark patterns" in advertising may be

[54] Available at: URL: https://ai.gov.ru/knowledgebase/etika-i-bezopasnost-ii/2023_eticheskie_rekomendacii_po_primeneniyu_rekomendatelynyh_tehnologiy_i_algoritmov_osnovannyh_na_iskusstvennom_intellekte_v_cifrovyh_servisah_alyyans_v_sfere_iskusstvennogo_intellekta/ (accessed: 10.10.2024)

recognized as improper advertising) and will not cover the whole concept of prohibition of user design that is misleading.

Properly used new technologies can serve the greater good and provide benefits for all subjects of economic activity. During the study the authors concluded that regulation could derive not from banning negative practice but from promoting positive one.

Having examined Russian online marketplaces, the authors summarized their user interface design practices and formulated the concept of "light patterns," which is the opposite of unfair manipulative techniques and are user-friendly.

As elements of ethical user interface design, "light patterns" encourage the user to make a conscious choice, which is particularly important when they are making an economic or legally binding decision.

This concept was presented to a committee of the Big Data Association, the organization that is working out the Code of Ethics for Data Use. The proposal was unanimously accepted by the members of the Big Data Association, Russian tech companies, including Yandex, Sberbank, Megafon, T-Bank, etc., and was included in the Big Data Association's White Paper — a set of best practices of fair data use.

The following "light patterns" were defined:

clarification: additional steps or clarifying barriers to confirm intent in economic or legally binding actions;

price Transparency: clear indication of the final price of the contents in a shopping cart including packaging, delivery and other paid options; the initial price of the order doesn't differ from the final price that the user sees when paying for the order, as it includes all options;

navigation: links are visually distinct from regular text elements, have a consistent style and are in a highly readable print;

reasonable highlighting: in the case of a choice between two categories, one of that could result in economic or legally binding consequences (acceptance of cookies, account registration, paid subscription etc.), it is necessary to highlight only the choice that does not provide such consequences or not to highlight any of them.

Undoubtedly, the passing of these recommendations indicates an intention of the Russian business to follow a positive practice that protect both the balance of interests of economic entities and the consumer as the weaker party in commercial relationship.

The development and implementation of this case study in the practice of the Russian companies will allow them to avoid legal and reputational risks and create a basis for the further legislative regulation.

Conclusion

The regulation of manipulative methods in the digital space is becoming an important task to ensure fair interaction between business and consumers. The study shows that, unlike foreign countries, where law enforcement practice regarding "dark patterns" is actively developing, Russia still lacks specific norms that fully cover this phenomenon. However, several provisions of the legislation can be applied to manipulative interfaces. The approving of ethical standards and the introduction of the concept of so-called "light patterns", based on fair interaction with users, may be the first step towards the formation of a legislative framework. In the long term, this will not only increase trust in digital services, but also reduce the risks for companies seeking to maintain a balance between the interests of all participants in the digital economy.

References

1. Blazheev V.V., Egorova M.A. (2020) Digital Law: textbook. Moscow: Prospect, 640 p. (in Russ.)

2. Brenncke M. (2024) Regulating Dark Patterns. *Notre Dame Journal of International and Comparative Law*, vol. 14, issue 1, pp. 39–79.

3. Calo R. (2014) Digital Market Manipulation. *The George Washington Law Review,* vol. 82, no. 4, pp. 995–1051.

4. Duplyakin V.M., Knjazheva Y.V. (2016) Checkout area service simulation of trade enterprise. *International Research Journal*, vol. 9, pp. 36–39. DOI: 10.18454/IRJ.2016.51.100

5. Hartzog W. (2018) *Privacy's Blueprint: The Battle to Control the Design of New Technologies.* Cambridge (Mass.): Harvard University Press, 384 p.

6. King J., Stephan A. (2021) Regulating Privacy Dark Patterns in Practice — Drawing Inspiration from California Privacy Rights Act. *Georgetown Law Technology Review*, vol. 5, issue 1, pp. 251–276.

7. Leiser M., Santos C. (2023) Dark Patterns, Enforcement, and the Emerging Digital Design Acquis: Manipulation beneath the Interface. *European Journal of Law and Technology*, vol.15, no.1, pp. 1–31.

8. Leiser M.R., Caruana M. (2021) Dark Patterns: Light to be found in Europe’s Consumer Protection Regime. *Journal of European Consumer and Market Law*, vol. 10, no. 6, pp. 237–251.

9. Luguri J., Strahilevitz L.J. (2021) Shining a Light on Dark Patterns. *Journal of Legal Analysis*, vol. 13, issue 1, pp. 43–109.

10. Nousiainen K., Ortega C.P. (2024) Dark Patterns in Law and Economics Framework. *Loyola Consumer Law Review,* vol. 36, issue 1, pp. 90–120.

11. Sharma S.J., Sharma I. (2023) Dark Patterns in a bright world: An analysis of the Indian Consumer Legal Architecture. *International Journal on Consumer Law and Practice*, vol. 11, pp. 123–146.

12. Solove D.J., Hartzog W. (2014) The FTC and the New Common Law of Privacy. *Columbia Law Review*, vol. 114, pp. 583–676.

13. Webb E. (2022) *Doomsday Algorithm. How Facebook, Google, Microsoft, Microsoft, Apple and other corporations create artificial intelligence and why it will lead to disaster*. Moscow: Eksmo, 400 p. (in Russ.)

14. Yablonski D. (2022) *Laws of UX-design*. Saint Petersburg: BXV- Petersburg:, 160 p.

15. Zuboff S. (2022) *The Era of Supervisory Capitalism. The battle for human future on the new frontiers of power*. Moscow: Gaidar Institute, 784 p. (in Russ.)

Information about the authors:

B.A. Edidin — Candidate of Sciences (Law), Deputy Director General for Legal Affairs.
K.V. Kochetkova — Candidate of Sciences (Law), Senior Lecturer, Senior Associate.
N.D. Sarankina — PhD Researcher, Junior Associate.

Contribution of the authors: the authors contributed equally to this article.
The authors declare no conflicts of interests.

The article was submitted to editorial office 05.10.2024; approved after reviewing 04.11.2024; accepted for publication 04.11.2024.