mathematics

MDPI

Article

Clustering of Dark Patterns in the User Interfaces of Websites and Online Trading Portals (E-Commerce)

Dmitry Nazarov [1,*] and Yerkebulan Baimukhambetov[2,3]

[1] Department of Business Informatics, Ural State University of Economics, 620144 Ekaterinburg, Russia
[2] Head of the Institutional Effectiveness, Abai University, Almaty 050010, Kazakhstan
[3] DBA Program, Kazakh-British Technical University, Almaty 050010, Kazakhstan
* Correspondence: slup2005@mail.ru

Abstract: dark patterns in the interfaces of users using sites and portals of online trading affect their behavior by companies that own digital resources. The authors propose to implement the detection of dark patterns on sites in user interfaces using cluster analysis algorithms using two methods for clustering many dark patterns in application interfaces: hierarchical and k-means. The complexity of the implementation lies in the lack of datasets that formalize dark patterns in user interfaces. The authors conducted a study and identified signs of dark patterns based on the use of Nelsen's antisymmetric principles. The article proposes a technique for assessing dark patterns using linguistic variables and their further interval numerical assessment for implementing cluster data analysis. The last part of the article contains an analysis of two clustering algorithms and an analysis of the methods and procedures for applying them to clustering data according to previously selected features in the RStudio environment. We also gave a characteristic for each resulting cluster.

Keywords: dark pattern; classification; clustering algorithms; user interface

MSC: 91B82; 91B86

check for updates

Citation: Nazarov, D.; Baimukhambetov, Y. Clustering of Dark Patterns in the User Interfaces of Websites and Online Trading Portals (E-Commerce). *Mathematics* **2022**, *10*, 3219. https://doi.org/10.3390/math10183219

Academic Editor: María del Carmen Valls Martínez

Received: 26 July 2022
Accepted: 25 August 2022
Published: 6 September 2022

Publisher's Note: MDPI stays neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Copyright: © 2022 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (https://creativecommons.org/licenses/by/4.0/).

1. Introduction

Trade relations always included the principles associated with persuading a potential client of the need to purchase a particular product. People used various ways to impose additional options and manipulate the behavior of the client. The goal was to increase the organization's profit per purchase (customer) through psychological methods of managing customer behavior.

The spread of digital technologies in trade and the service sector in modern conditions has new opportunities to influence the behavior of the client and get more profit. The principles of trade relations and methods of persuasion have been transferred to digital platforms, the user interfaces of which contain "dark patterns". Such patterns influence people's behavior, for example, for commercial or political purposes. The number of websites and mobile applications is constantly growing, and their digital architecture and interface design have a powerful influence on human behavior and decision-making. The authors of various scientific articles have raised this issue, considering the design of interfaces over the past 10 years.

Since we associate the use of dark patterns with user interface design, we can name two Danish engineers Jakob Nielsen and Rolf Molich as the founders of this area of activity. In 1990, they planned 10 principles that a user-friendly interface should comply with [1–5]. From this point of view, "dark patterns" are a vivid example of ignoring these principles, "dark patterns" are interfaces created based on Nielsen's antisymmetric principles.

The number of dark patterns in user interfaces has increased in recent years, so the amount of damage caused to consumers has also increased. The number of various scientific papers devoted to various aspects of the detection, research, and classification

of dark patterns has also increased. We would like to note the studies [6–16], in which the authors consider the problem of using dark patterns in user interfaces from different points of view. We present the references list in historical-logical order. The number of publications is growing non-linearly and we see some progress in the scientific interest in this problem; this emphasizes the relevance of the study.

Perhaps the most successful attempt to classify dark patterns is the deceptive design [1,2] (formerly darkpatterns.org), which is owned by Harry Brignull, an independent user interface designer based in London. Harry Brignull is compiling a unique collection of dark patterns—real examples of how designers and businesses use specific web design techniques to deceive Internet users and encourage them to take action.

Economics Nobel Prize winners Daniel Kahneman and Amos Tversky indirectly looked at dark patterns in terms of how they affect people's behavior; they identified and formalized the psychological principles and criteria for decision-making and the risks associated with them [17].

The trend associated with the introduction of digital platforms in all areas of the economy stimulates the appearance of dark patterns in application interfaces and increases the number of their types, so it will take more time and effort on the part of users to detect dark patterns. In addition, practically no such studies have been conducted in the Russian segment of the Internet; this is due to the lack of data and methods for their formalization. In general, I would like to note that while in the world the classification of dark patterns is carried out on the basis of expert assessments, therefore, a technique is required to automate this process. Our article proposes an approach that allows us to automate the process of extracting types of dark patterns to some extent.

The purpose of the article is to cluster dark patterns in application interfaces using the R language based on user data and criteria developed by the authors.

Dark patterns in application interface are the object of research.

The subject of the study is classifying dark patterns in application interfaces using clustering algorithms implemented in the R language.

The article is divided into 4 parts. The first part contains a detailed analysis of the literature on various issues of using dark patterns in user interfaces. In the second part, the authors discuss existing approaches to the classification of dark patterns in various scientific studies. The third part of the article describes the data preparation model for the clustering procedure. In the fourth part, a cluster analysis of data on the use of dark patterns in application interfaces is carried out, with an emphasis on Russian-language content. In conclusion, conclusions are drawn and prospects for the study are discussed.

2. Using Dark Patterns in Application Interfaces

Dark patterns are user interfaces whose designers deliberately confuse users, make it difficult for users to express their actual preferences, or manipulate users into taking certain actions. The goal of most dark patterns is to manipulate the consumer into taking actions that are inconsistent with their preferences, as opposed to marketing efforts to change those preferences.

In terms of Kahnemann et al., "dark patterns" encourage users to decide using "System 1" based on an intuitive approach, rather than thinking through decisions using "System 2" based on cognitive features of decision-making.

We associate the first wave of academic research on dark patterns with the formalization of this phenomenon and the development of the first typologies of dark patterns [1–9].

The authors of most studies focus on user interfaces, including the location of windows, buttons, titles, and other elements on application screens [3,4,12]. José P Zagal et al. explore the features of using dark patterns on game portals [4,7]. Studies [6,9] consider the psychological basis for the use of dark patterns. The works [10,12,14] contain legal content devoted to dark patterns.

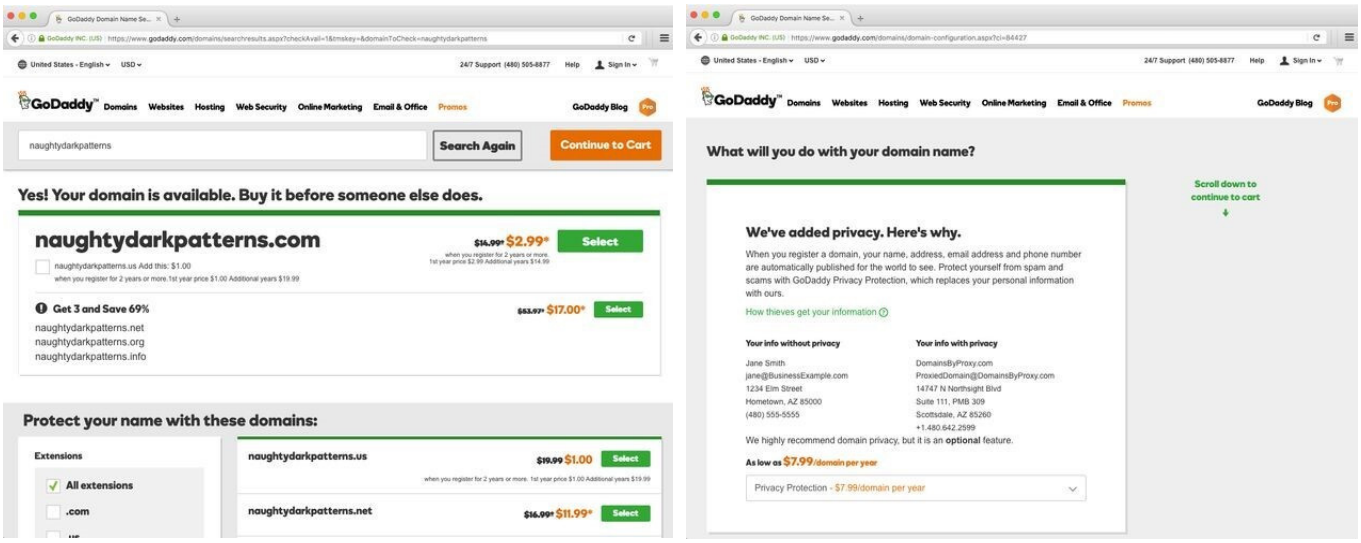
Arunesh Mathur and co-authors published a voluminous academic study on the prevalence of dark patterns and proposed a semi-automated method for scanning over

11,000 popular shopping sites. The written script allowed them to get interesting results: over 11% of sites contained certain types of dark patterns [13]. The modern trend in the study has shifted towards mobile applications. Most of the works of 2020–2021 explore the features of using dark patterns in mobile applications and social networks [18–28].

We see a pop-up in the Instagram app asking, "Do you want the service to use your actions in the app and on the website to provide better ad quality?". Two types of response for the user: a button with a slightly darker shade of black than the background of the popup, which allows "Make ads less personalized", and a bright blue button that calls for "Make ads more personalized" [5,29].

The number of dark patterns multiplied during the COVID-19 pandemic. Most purchases are made online. The most common way to control people's behavior has become the way when buying food, air and railway tickets, services of various kinds, and adding services to the basket that the user would not like to add; this method is used not only for beginners or inexperienced users; it is successfully used for advanced users [11].

Godaddy.com sells domain names and uses a dark pattern: «Get 3 and save 69%» for USD 17.00. The next page adds privacy protection automatically to your shopping cart for USD 7.99 (Figure 1a,b).



(**a**)First Step purchase. (**b**) Last Step purchase

Figure 1. «Add to cart» dark pattern on godaddy (https://www.godaddy.com/. accessed on 12 May 2022).

The purchase price is quadrupled to USD 154.31 because there were a few extras tucked into the shopping cart—2 years of domain registration for all four domains (instead of one year as listed in the price list on the front page) and privacy protection; this scheme is one of the most common among all dark patterns.

There are similar dark patterns on many Russian-language sites and portals related to the sale of air and railway tickets, where insurance is imposed on potential customers, payment for SMS messages about force majeure, etc. Sales services of Aeroflot, Pobeda, Russian Railways, planning portals travel from Tinkoff, Ostrovok, etc. we can give as an example.

If we assume that only 1% of 1000 customers do not notice dark patterns, then godaddy.com will earn not USD 17,000 but about USD 1370 more; this is good for the company but bad for the customer.

If the first wave of research created a useful classification of dark patterns in user interfaces, then the second wave allowed us to establish the growing prevalence of dark pattern types, and also automated recognizing dark patterns in user interfaces to some extent. The directions of scientific search research are diverse, and, on the one hand, scientists evaluate the effectiveness of dark patterns in persuading customers, on the other

hand, they are trying to develop measures to protect users from using dark patterns in online trading. If society wants to understand the scale of the problem and the feasibility of their regulation, then these and related issues should be important.

From the point of view of the concept of symmetry, dark patterns are a certain asymmetry that occurs in the process of online trading; this asymmetry lies in the fact that the owners of online trading applications know more about the purchase process (not about the product, as in the classical theory) than users do, and this leads to the fact that a potential client when buying a product or service, pays more than they would like.

3. Classification of Dark Patterns

By going to the «Types of deceptive design» page of the Deceptive design service, you can get acquainted with the classification of dark patterns [1]:

1. «Trick questions»—by filling out a form, you answer a question that tricks you into giving an answer you didn't want. On a cursory glance at the question, it seems to ask one thing, but on closer reading, it is asking quite another;
2. «Sneak into basket»—you're trying to buy something, but somewhere along the way, the site adds an item to your cart, often via an opt-out switch or a checkbox on the previous page;
3. «Roach motel»—you get into a situation easily but then it is difficult for you to get out of it (for example, a premium subscription);
4. «Privacy zuckering»—they tricked you into publicly sharing more information about yourself than you intended. Named after Facebook CEO Mark Zuckerberg;
5. «Price comparison prevention»—the seller prevents you from comparing the price of the product with another product, so you cannot make an informed decision;
6. «Misdirection»—design focuses your attention on one thing to divert attention from another;
7. «Hidden costs»—you get to the last step of the checkout process but find some unexpected charges like shipping, tax, etc.;
8. «Bait and switch»—you intend to do one thing but something else happens;
9. «Confirmshaming»—the user's fault for choosing something. The opt-out option is worded in such a way as to shame the user;
10. «Disguised ads»—ads disguised as other content or navigation to get you to click on them;
11. «Forced continuity»—when your free trial ends and your credit card is being charged insanely; this is exacerbated because unsubscribing becomes difficult in some cases;
12. «Friend spam»—a site or other web service that asks you to access email or social media under the pretense of using it for the desired result (such as finding friends) but then spamming all of your contacts in a message.

We have given a classification of all existing and noticed scientists' dark patterns that are used in the interfaces of various web services. On the one hand, some dark patterns from the above classification cannot be automatically recognized and included in some predictive systems, on the other hand, some types of dark patterns in the above classification are similar and can be considered as variations of the same type of dark patterns; it is necessary to cluster the data array on dark patterns, but here there is a difficulty in the absence of datasets with selected features (predictors) of dark patterns. Below, we will present an approach that will allow us to build a new classification of dark patterns and simplify the writing of service for intelligent recognition of dark patterns.

4. Model of Data Preparation for the Procedure of Clustering Dark Patterns Based on Expert Assessment

Clustering (or cluster analysis) is partitioning a set of objects into groups called clusters. Within each group, there should be "similar" objects, and objects of different groups should be different [30]. The application of cluster analysis includes the following steps:

- selection of a sample of objects for clustering;

- determination of the set of variables by which the objects in the sample will be evaluated. Normalization of variable values, if necessary;
- calculation of similarity measure values between objects;
- application of the cluster analysis method to create groups of similar objects (clusters);
- presentation of the results of the analysis [31];

To get data for cluster analysis, we selected 152 sites from various sources with dark patterns and chose 20 people—students of the study program «Business informatics» and «Information security» at the Ural State University of Economics (Yekaterinburg). We used linguistic variables to exclude the subjectivity of ratings as a rating scale. Each respondent had to evaluate a certain number of sites from the sample according to several criteria we obtained these signs during the analysis of 10 heuristic principles of Nielsen. We have identified 10 antisymmetric principles that show dark patterns. Many features are common to several patterns at once. Based on the listed signs, we can select several significant ones. Using the DEMATEL and MICMAC methods, we excluded five features [32–35].

Signs of dark patterns in the interface:

- complicated interface (ID);

This concept includes a non-obvious interface, small print, and not noticeable explanations;

- data leak (UD);

A sign of an interface where the user presents more information about himself to companies than he really would like;

- cost increase (US);

The sign is typical for dark patterns, where the client, one way or another, will spend more money;

- impossibility to refuse (UO);

The opportunity to refuse everything exists formally; however, not every user can notice an additional option when making a purchase and inadvertently take an action that he would not like to do;

- hidden advertising (UA);

The sign is typical for patterns that do not force the user to pay money directly, but indirectly have some psychological effect on him, which contributes to the acquisition of additional goods or services.

Scale:

- no sign of a dark pattern in the interface (Z);
- low presence of a dark pattern in the interface (L);
- uncertainty of finding a feature in a dark pattern (N);
- influential presence of a dark pattern in the interface (H);
- dark pattern is always present in the interface (F);

Thus, any site under study (S) from the list was encoded with a tuple G (1):

$$S = G\ (ID, UD, US, UO, UA), \quad (1)$$

Experts, using a linguistic scale built with the help of fuzzy set theory, had to give their marks for a particular instance of the site. We can present the result of their work for the i-th site containing a dark pattern as follows (2):

$$S_i = G(ID_i = N, UD_i = H, US_i = F, UO_i = Z, UA_i = L) \quad (2)$$

It is known that implementing cluster analysis of data requires numerical values of features, so we assigned a certain numerical value to each linguistic variable based on the interval scales used in fuzzy set theory and expert assessment methods [36–41]. Since nothing is known about the distribution of values of linguistic variables within the interval,

we decided [42,43], by the theory of fuzzy sets, to consider the value of a linguistic variable as a triangular number, where the maximum value of the membership function lies in the middle of the interval (Table 1). Our assumption was completely confirmed after receiving the clustering results.

Table 1. Numerical values of linguistic variables of the interval scale.

Linguistic Variable	Value Interval [0;10]	Interval Midpoint	The Value of the Membership Function [0;1]
no sign of a dark pattern in the interface (Z)	0	0	0
low presence of a dark pattern in the interface (L)	[2;4]	3	0.3
uncertainty of finding a feature in a dark pattern (N)	5	5	0.5
Continuation of Table 1.			
an influential presence of a dark pattern in the interface (H)	[6;10]	8	0.8
a dark pattern is always present in the interface (F)	10	10	1

The peculiarity of this approach is that when we get an unsatisfactory result of the value of the membership function, we can redefine and re-execute the clustering algorithm. A more subtle approach to determining the center of a triangular number.

The following estimates were obtained because of processing the data of the respondents. Table 2 shows these results.

Table 2. Respondents' assessment of presence of signs of dark patterns on websites and portals of online trading.

	Dark Patterns	Data Leak	Cost Increase	Complicated Interface	Hidden Advertising	Impossibility to Refuse
1	Trick questions (12)	0.1	0.5	1	0	1
2	Sneak into basket (14)	0	1	0.8	0.1	0
3	«Roach» motel (10)	0.1	0.5	1	0	0.8
4	Privacy zuckering (15)	1	0	0.5	0.1	0.5
5	Price comparison prevention (11)	0	1	0.8	0.1	0
6	Misdirection (14)	0	1	0.8	0.5	0.1
7	Hidden costs (15)	0	1	0.8	0	0
8	Bait and switch (17)	0.1	0.5	1	0	1
9	Confirmshaming (14)	0.1	0.5	1	0.8	1
10	Disguised ads (11)	0.1	0.5	1	1	1
11	Forced continuity (10)	0	1	0.8	0.1	0.5
12	«Friend» spam (12)	1	0.1	0.5	0.1	0.5

The number of sites from the sample with dark patterns is in Table 2 in the second column in brackets; these data show the balance of the sample regarding the classified dark patterns on online trading sites.

5. Implementation of Cluster Analysis Using the R Language in the RStudio Environment

We will carry out cluster data analysis using two methods (k-means and hierarchical cluster analysis), which will allow us to accurately determine the differences between clusters and establish their number with a certain accuracy [32,33].

After importing the data into RStudio and preparing it for the cluster analysis procedure, it is necessary to determine the optimal number of clusters; this is achieved using the fviz_nbclust() function.

The fviz_nbclust() function supports several methods for finding the optimal number of clusters: «silhouette» (average silhouette width), «wss» (sum of squared distances), «gap_stat» (gap statistics). Figures 2–4 show the result of all three methods.

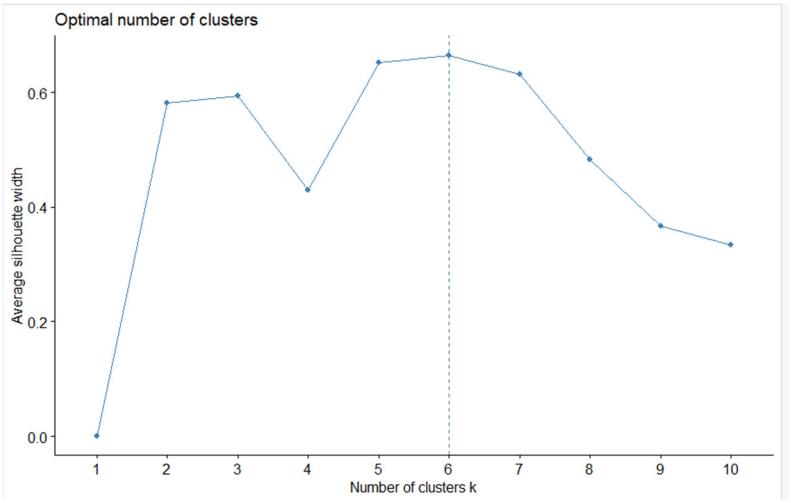


Figure 2. Results of applying the "silhouette" method to the data.

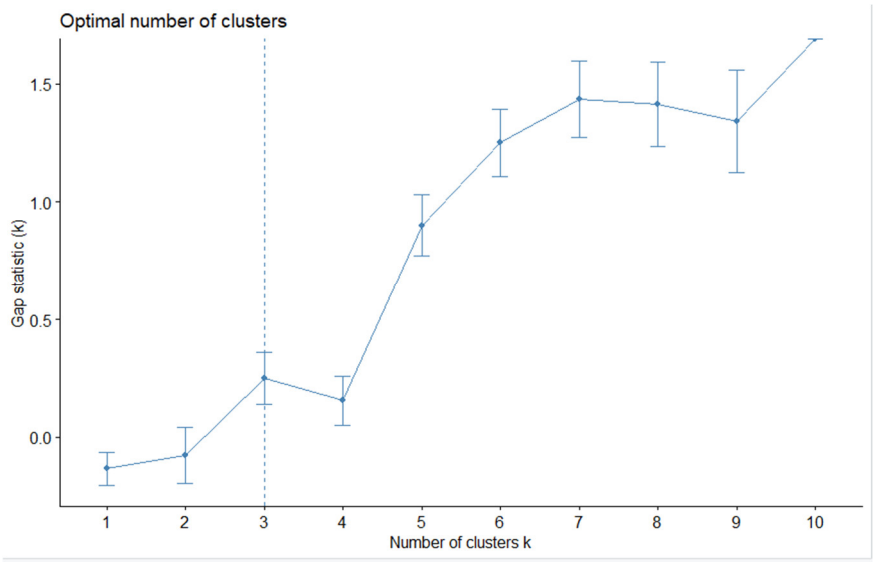


Figure 3. Results of applying the "wss" method to the data.

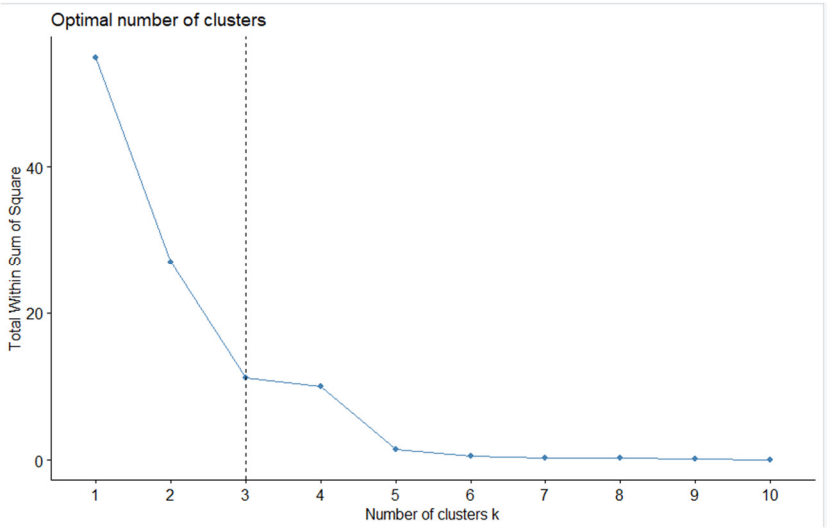


Figure 4. Results of applying the "gap_stat" method to the data.

An analysis of the results obtained shows that the "silhouette" method did not cope well with the optimization problem, highlighting 6 clusters. The resulting graph (see Figure 2) erroneously suggests 6 clusters as the optimal number. We will show this later.

First, apply the k-means method to cluster the results.

The result of the performed manipulations is Figure 5, which presents the results of cluster analysis.

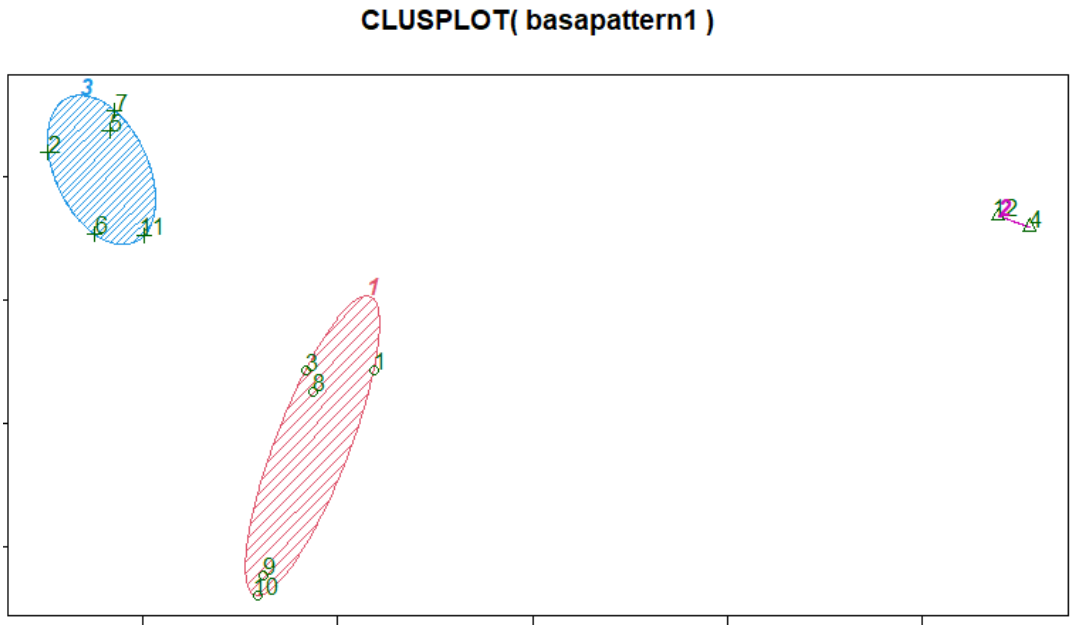


Figure 5. Clustering of the initial data by the k-means method.

The result of applying hierarchical cluster analysis became dendrograms (Figures 6 and 7).

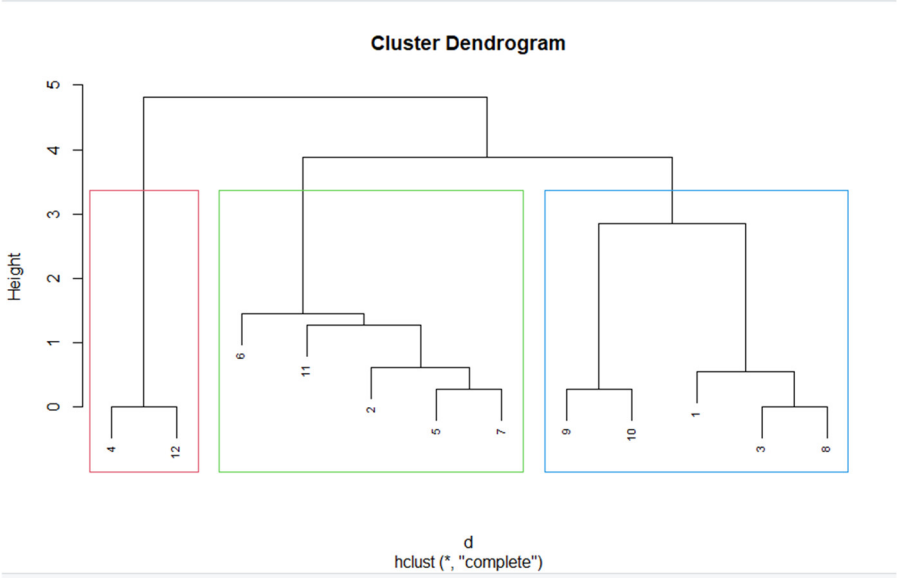


Figure 6. Dendrogram ("complete" method). *—hclust command options.

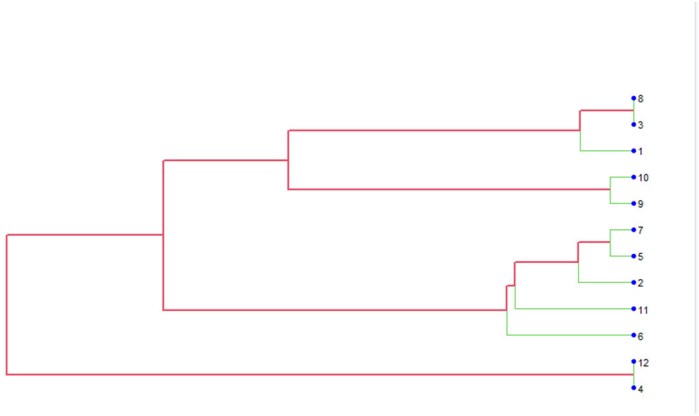


Figure 7. Dendrogram (method "ward.D2").

Analyzing the results of clustering, we conclude they are identical.

Using the method of hierarchical cluster analysis, we will divide into 6 clusters, which was recommended by the "silhouette" optimization method. Figure 8 shows the result.

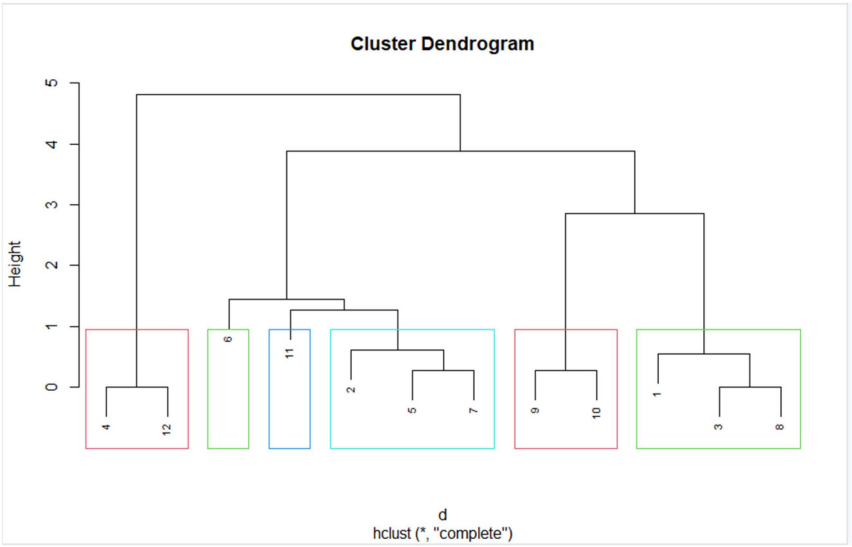


Figure 8. The result of hierarchical clustering into 6 clusters. *—hclust command options.

The analysis of the obtained dendrogram shows that the 6th and 11th types of dark patterns are in separate clusters, although it is visible that we can combine them with the 2, 5, 7 types of dark patterns.

We would like to note that the use of several clustering methods, methods for calculating distances, and determining the optimal number of clusters is a necessity when implementing the data clustering process; this is because the clustering algorithm always gives the result—splitting the data into clusters, even when there are no actual clusters. The application of several methods confirms the obtained results.

We can conclude that in this case, there are three clusters.

The first cluster includes the following dark patterns:

- confirmationshaming;
- disguised ads;
- «roach motel»;
- bait and switch;
- trick questions;

The second cluster includes the following dark patterns:

- privacy zuckering;
- «friend» spam;

The third cluster includes the following dark patterns:

- price comparison prevention;
- hidden costs;
- sneak into basket;
- misdirection;
- forced continuity.

If we turn to the definition of the dark patterns in the existing classification, then the cluster analysis of the data helped to identify 3 clusters that combine dark patterns that are similar in meaning.

Next, we analyzed the websites of Aeroflot (3) and Tinkoff Bank (4).

$$S_a = G\ (ID_a = 0,\ UD_a = 0.9,\ US_a = 0.9,\ UO_a = 0.3,\ UA_a = 0.5) \quad (3)$$

$$S_t = G\ (ID_t = 0, UD_t = 1,\ US_t = 0.5,\ UO_t = 0.9,\ UA_t = 0.5) \quad (4)$$

Dark patterns were found on these sites, and according to the results of cluster analysis, they belong to the third cluster of our classification.

6. Conclusions

The authors of the article analyzed the existing classification of dark patterns in the application interface of users of online services and Internet commerce, gave their chief characteristics, and provided examples. All types of dark patterns were sorted into three clusters based on the selected features. Based on the 10 Nelsen principles of building a user-friendly interface, the authors first formed 10 antisymmetric principles that characterize dark patterns and then they combined them using the DEMATEL and MICMAC expert methods into five features that describe each type of dark pattern.

The article presents a method for preparing data for cluster analysis, based on the linguistic assessments of respondents from a set of 152 sites containing dark patterns.

In the last section of the article, we implemented several clustering algorithms with different parameters using the R language libraries in the Rstudio environment and showed the optimal number of clusters into which the initial sample of data obtained from the survey of respondents is divided.

Because of the work done, we obtained three clusters into which the existing dark patterns were combined. According to the logic of cluster analysis, we have given a characteristic of each cluster.

The characteristic of the first cluster, which combines the dark patterns 1, 3, 8, 9, 10, is associated with the use of a complex interface, an incomprehensible arrangement of windows, switches, confirmations of certain actions, and the impossibility of canceling them. We classify them as veiled fraudulent activities.

The characteristic of the second cluster, which combines the dark patterns 4 and 12, is associated with a violation of user data confidentiality. Such sites require special attention from regulators and law enforcement agencies, up to a complete ban on the use of such interfaces in Internet commerce.

The third cluster, which includes types of dark patterns 2, 5, 6, 7, 11, is associated with extracting additional profit by explicitly or implicitly imposing additional services, and monthly debiting of funds from users' cards. Such sites offer nothing illegal, and therefore the user of Internet trading sites must know and follow several rules when using their interfaces.

We have identified features that characterize dark patterns in user interfaces; they can be successfully formalized, and based on them, a fairly simple program code can be obtained, which can later be used as the basis for a site analysis service for dark patterns.

As a continuation of scientific research in this direction, I would like to propose, based on the constructed model, to develop software that would identify dark patterns in user

interfaces using machine learning methods, and indeed, we are already developing such developments. Machine learning methods will also make it possible to identify frequently used types of dark patterns in application interfaces.

Author Contributions: Data curation, D.N.; Formal analysis, D.N.; Resources, Y.B.; Supervision, D.N.; Validation, Y.B.; Visualization, Y.B. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Brignull, H. Dark Patterns. 2018. Available online: https://darkpatterns.org/ (accessed on 9 September 2020).
2. Hanson, J.D.; Kysar, D.A. Taking behavioralism seriously: The problem of market manipulation. *NYUL Rev.* **1999**, *74*, 630.
3. Conti, G.; Sobiesk, E. Malicious Interface Design: Exploiting the User. In *Proceedings of the 19th International Conference on World Wide Web (WWW '10), Raleigh, NC, USA, 26–20 April 2010*; Association for Computing Machinery: New York, NY, USA, 2010; pp. 271–280. [CrossRef]
4. Zagal, J.P.; Björk, S.; Lewis, C. Dark patterns in the design of games. In *Foundations of Digital Games 2013*; Society for the Advancement of the Science of Digital Games: Santa Cruz, CA, USA, 2013; p. 8.
5. Hannak, A.; Soeller, G.; Lazer, D.; Mislove, A.; Wilson, C. Measuring Price Discrimination and Steering on E-Commerce Web Sites. In *Proceedings of the 2014 Conference on Internet Measurement Conference (IMC '14), Vancouver, BC, Canada, 5–7 November 2014*; Association for Computing Machinery: New York, NY, USA, 2014; pp. 305–318. [CrossRef]
6. Greenberg, S.; Boring, S.; Vermeulen, J.; Dostal, J. Dark Patterns in Proxemic Interactions: A Critical Perspective. In *Proceedings of the 2014 Conference on Designing Interactive Systems (DIS '14), Vancouver, BC, Canada, 21–25 June 2014*; ACM: New York, NY, USA, 2014; pp. 523–532. [CrossRef]
7. Lewis, C. *Irresistible Apps: Motivational Design Patterns for Apps, Games, and Web-Based Communities*, 1st ed.; Apress: Berkely, CA, USA, 2014.
8. Bösch, C.; Erb, B.; Kargl, F.; Kopp, H.; Pfattheicher, S. Tales from the Dark Side: Privacy Dark Strategies and Privacy Dark Patterns. *Proc. Priv. Enhancing Technol.* **2016**, *4*, 237–254. [CrossRef]
9. Lazar, J.; Feng, J.H.; Hochheiser, H. *Research Methods in Human-Computer Interaction*; Morgan Kaufmann: Boston, MA, USA, 2017.
10. Frobrukerrådet. *Deceived by Design: How Tech Companies Use Dark Patterns to Discourage Us from Exercising Our Rights to Privacy*; Frobrukerrådet: Oslo, Norway, 2018.
11. Gray, C.M.; Kou, Y.; Battles, B.; Hoggatt, J.; Toombs, A.L. The Dark (Patterns) Side of UX Design. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems (CHI '18), Montreal, QC, Canada, 21–26 April 2018*; ACM: New York, NY, USA, 2018; p. 14. [CrossRef]
12. Hartzog, W. *Privacy's Blueprint: The Battle to Control the Design of New Technologies*; Harvard University Press: Cambridge, MA, USA, 2018.
13. Mathur, A.; Acar, G.; Friedman, M.J.; Lucherini, E.; Mayer, J.; Chetty, M.; Narayanan, A. Dark Patterns at Scale: Findings from a Crawl of 11K Shopping Websites. *Proc. ACM Hum. Comput. Interact.* **2019**, *3*, CSCW. [CrossRef]
14. Warner, M.; Fischer, D. Senators Introduce Bipartisan Legislation to Ban Manipulative "Dark Patterns". Available online: https://www.fischer.senate.gov/public/index.cfm/2019/4/senators-introduce-bipartisan-legislation-to-ban-manipulative-dark-patterns (accessed on 9 September 2020).
15. Lacey, C.; Caudwell, C. Cuteness as a 'Dark Pattern' in Home Robots. In *Proceedings of the 14th ACM/IEEE International Conference on Human-Robot Interaction (HRI '19), Daegu, Korea, 11–14 March 2019*; IEEE Press: Piscataway, NJ, USA, 2019; pp. 374–381.
16. Utz, C.; Degeling, M.; Fahl, S.; Schaub, F.; Holz, T. (Un)Informed Consent: Studying GDPR Consent Notices in the Field. In *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security, (CCS '19), London, UK, 11–15 November 2019*; Association for Computing Machinery: New York, NY, USA, 2019; pp. 973–990. [CrossRef]
17. Tversky, A.; Kahneman, D. Prospect theory: An analysis of decision under risk. *Econometrica* **1979**, *47*, 263–291.
18. Day, G.; Stemler, A. Are Dark Patterns Anticompetitive? *Ala. Law Rev.* **2020**, *72*, 1–45. [CrossRef]
19. Di Geronimo, L.; Braz, L.; Fregnan, E.; Palomba, F.; Bacchelli, A. UI Dark Patterns and Where to Find Them: A Study on Mobile Applications and User Perception. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems (CHI '20), Honolulu, HI, USA, 25–30 April 2020*; Association for Computing Machinery: New York, NY, USA, 2020; pp. 1–14. [CrossRef]
20. Hurwitz, J. Designing a Pattern, darkly. *NCJL Technol.* **2020**, *22*, 57.

21. Luguri, J.; Strahilevitz, L.J. Shining a Light on Dark Patterns. *J. Leg. Anal.* **2021**, *13*, 43–109. Available online: https://academic.oup.com/jla/article/13/1/43/6180579 (accessed on 28 May 2022). [CrossRef]
22. Machuletz, D.; Böhme, R. Multiple purposes, multiple problems: A user study of consent dialogs after GDPR. *Proc. Priv. Enhancing Technol.* **2020**, *2*, 481–498. [CrossRef]
23. Maier, M.; Harr, R. Dark Design Patterns: An End-User Perspective. *Hum. Technol.* **2020**, *16*, 170–199. [CrossRef]
24. Narayanan, A.; Mathur, A.; Chetty, M.; Kshirsagar, M. Dark Patterns: Past, Present, and Future. *Queue* **2020**, *18*, 67–92. [CrossRef]
25. Nouwens, M.; Liccardi, I.; Veale, M.; Karger, D.; Kagal, L. Dark Patterns after the GDPR: Scraping Consent Pop-Ups and Demonstrating Their Influence. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems (CHI '20), Honolulu, HI, USA, 25–30 April 2020*; Association for Computing Machinery: New York, NY, USA, 2020; pp. 1–13. [CrossRef]
26. Soe, T.H.; Nordberg, O.E.; Guribye, F.; Slavkovik, M. Circumvention by Design—Dark Patterns in Cookie Consent for Online News Outlets. In *Proceedings of the 11th Nordic Conference on Human-Computer Interaction: Shaping Experiences, Shaping Society (NordiCHI '20), Tallinn, Estonia, 25–29 October 2020*; Association for Computing Machinery: New York, NY, USA, 2020; p. 12. [CrossRef]
27. Waldman, A.E. Cognitive biases, dark patterns, and the 'privacy paradox. *Curr. Opin. Psychol.* **2020**, *31*, 105–109. [CrossRef] [PubMed]
28. Dark Patterns, the Tricks Websites Use to Make You Say Yes, Explained. Available online: https://vox.com/recode/22351108/dark-patterns-ui-web-design-privacy (accessed on 28 May 2022).
29. Anderberg, M. *Cluster Analysis for Applications*; Academic Press: Cambridge, MA, USA, 1973.
30. Kaufman, L.; Rousseeuw, P. *Finding Groups in Data: An Introduction to Cluster Analysis*; Wiley-Interscience: Hoboken, NJ, USA, 2005.
31. Khan, S.S.; Ahmad, A. Cluster center initialization algorithm for kmeans clustering. *Pattern Recognit. Lett.* **2004**, *25*, 12931302.
32. Jassbi, J.; Mohamadnejad, F.; Nasrollahzadeh, H. A Fuzzy DEMATEL framework for modeling cause and effect relationships of strategy map. *Expert Syst. Appl.* **2011**, *38*, 5967–5973.
33. Chen, F.H.; Chi, D.-J. Application of a new DEMATEL to explore key factors of China's corporate social responsibility: Evidence from accounting experts. *Qual. Quant.* **2015**, *49*, 135–154.
34. Wu, H.H.; Chang, S.Y. A Case Study of Using DEMATEL Method to Identify Critical Factors in Green Supply Chain Management. *Appl. Math. Comput.* **2015**, *256*, 394–403.
35. Khanam, S.; Siddiqui, J.; Talib, F. Modelling the TQM Enablers and IT Resources in the ICT Industry: An ISM-MICMAC Approach. *Int. J. Inf. Syst. Manag.* **2015**, *1*, 195–218. [CrossRef]
36. Ahmad, A.; Dey, L. A k-mean clustering algorithm formixed numeric and categorical data. *Data Knowl. Eng.* **2007**, *63*, 503–527.
37. Miyamoto, S.; Huynh, V.; Fujiwara, S. Methods for clustering categorical and mixed data: An overview and new algorithms. In *Integrated Uncertainty in Knowledge Modelling and Decision Making*; Spinger: Cham, Switzerland, 2018; pp. 75–86.
38. Ahmad, A.; Dey, L. *Algorithm for Fuzzy Clustering of Mixed Data with Numeric and Categorical Attributes*; Springer: Berlin/Heidelberg, Germany, 2005; pp. 561–572.
39. Zhanbayev, R.; Sagintayeva, S.; Ainur, A.; Nazarov, A. The Use of the Foresight Methods in Developing an Algorithm for Conducting Qualitative Examination of the Research Activities Results on the Example of the Republic of Kazakhstan. *Mathematics* **2020**, *8*, 2024.
40. Nazarov, D.; Nazarov, A.; Kovtun, D. Building Technology and Predictive Analytics Models in the SAP Analytic Cloud Digital Service. In *Proceedings of the 2020 IEEE 22nd Conference on Business Informatics (CBI), Antwerp, Belgium, 22–24 June 2020*; Institute of Electrical and Electronics Engineers (IEEE): Piscataway, NJ, USA, 2020; Volume 2, pp. 106–110.
41. Nazarov, D.M.; Morozova, A.S.; Kokovikhin, A.Y. SAP Analytic Cloud: A Tool for the Formation of Professional Competencies of Business Analyst. In Proceedings of the CEUR Workshop, St. Petersburg, Russia, 17–20 June 2020; p. 2570.
42. Nazarov, D. Causality: Intelligent valuation models in the digital economy. *Mathematics* **2020**, *8*, 2174.
43. Nazarov, D.M. Classification of models and description of trends in assessing the causality of relationships in socio-economic processes. *Bus. Inform.* **2020**, *14*, 47–61. [CrossRef]