Dark Patterns in the Public Sector: A Study of Cookie Consent Interfaces on Croatian Websites

Marija Kuštelega
University of Zagreb Faculty of Organization and Informatics
Department of Information Systems Development
Pavlinska 2, 42000 Varaždin, Croatia
marija.kustelega@foi.unizg.hr

Abstract. *With the implementation of the General Data Protection Regulation (GDPR), it is now required to obtain explicit user consent before using any data about them. The way cookie consents are designed can directly affect an individual's ability to make an informed privacy decision. Because of this, a lot of websites use dark patterns, a term described as a visual pattern used to trick users into choosing options that are not in their best interests. To evaluate the presence of dark patterns in the public sector, a sample of the 100 most popular Croatian public sector websites, based on the Tranco list, was analyzed. This analysis found that over 96% of websites with cookie consent used some form of dark patterns. Although most of them have all the options listed that they should have according to the legal obligations, not all options are easily accessible, such as the ability to reject the consent with a single click. Providing users with easily understandable information, making it simple to accept or reject cookies, and allowing users to easily change their preferences are all components of good cookie consent design.*

Keywords. cookie consent, dark patterns, privacy

1 Introduction

Gartner hype-cycle for emerging technologies for 2024 has ranked delivering human-centric security and privacy as one of the four main themes (Gartner, 2024). This demonstrates how the focus is shifting from quick solution delivery to safe solution implementation, highlighting the importance of incorporating security and privacy measures into user interface design. One of the related initiatives is usable privacy and security research, focused on designing usable privacy interfaces to help users make better privacy decisions (Distler et al., 2021). Usable privacy researchers deal with various segments of privacy-related topics in the field of human-computer interaction, one of which is the provision of usable privacy notices (Fischer-Hübner and Karegar, 2024). Because dark patterns directly contradict these core principles, they have thus emerged as a highly interesting research topic.

Dark patterns, first introduced by Henry Brignull in 2010, attempted to explain how websites deceive users through their user interface (Alharbi, Albesher, and Wahsheh, 2023). It defines that: “Deceptive design patterns (also known as ‘dark patterns’) are tricks used in websites and apps that make you do things that you didn’t mean to, like buying or signing up for something” (Brignull et al., 2023).

Because dark patterns draw attention away from ethics, transparency, and fair business practices, they pose a serious threat to e-commerce websites in particular. Moreover, the European Directive 2005/29/EC on unfair commercial practices has recognized the dark pattern as a potential threat in the form of manipulative practices (European Commission, 2022). Other organizations, such as the Organization for Economic Co-operation and Development (OECD), also deal with this topic by trying to create a definition and taxonomy of dark patterns in order to be able to recognize the characteristics of dark commercial patterns (OECD, 2022).

However, other areas besides retail are also affected; more than 90% of 243 e-government websites have dark patterns in their user interfaces (Alharbi et al., 2023). Generally, dark patterns are common in European Union (EU) countries, where at least one dark pattern was present in 73 of 75 websites and apps studied (European Commission, 2022). A newer study conducted in June 2024 by the International Consumer Protection and Enforcement Network (ICPEN) showed that 76% of 642 websites and apps worldwide had some form of dark pattern, while nearly 67% used multiple combinations of dark patterns (ICPEN, 2024). Such data show that the situation has improved recently, but there is still a strong presence of dark patterns globally.

Usually, research was focused on popular domains such as e-commerce websites and news outlets (Mathur et al., 2019; Soe et al., 2020). There is a lack of research focused on public sector websites.

Public sector websites are expected to protect user privacy in order to uphold the integrity and sovereignty of public institutions in relation to private sector companies (Sørensen and Kosta, 2019). The aim of this research was to examine the extent to which public sector websites in Croatia employ dark patterns (manipulative design practices) to obtain user consent. The novelty of this research lies in the fact that no prior study has specifically examined public sector websites in this context. Research questions were as follows:

- Which categories of dark patterns are most commonly used in cookie consent interfaces present on public sector websites in Croatia?
- What additional characteristics of cookie consent interfaces should be improved to enhance user control (e.g., number of options, clicks needed to reject consent)?

The structure of this paper is as follows: Section 2 explains background and related work; Section 3 describes the utilized methodology for sampling websites; Section 4 presents the results of the analyzed dark patterns; Section 5 discusses the findings and concludes the work.

2 Background

2.1 Dark Patterns Categories

Dark patterns in terms of cookie consent interfaces can be described as any design practices that can lead users to unknowingly consent to data collection, which is not in line with their privacy preferences (Kitkowska, 2023). Colin Gray has made a comprehensive classification of dark patterns, putting them into five key categories: (1) Nagging, (2) Obstruction, (3) Sneaking, (4) Interface interference, and (5) Forced Action (Gray et al., 2018). In Table 1, key categories of dark patterns are briefly described with examples.

Table 1. Classification of dark pattern categories (Gray et al., 2018)

Dark pattern	Description	Example
Nagging	The user's desired task is interrupted by unrelated tasks.	Pop-ups, audio notices
Obstruction	The interaction is being made more challenging than it should be.	Unequal paths
Sneaking	An attempt to hide, mask, or delay the disclosure of relevant information.	Delayed disclosure of certain costs
Interface interference	Any kind of interface manipulation that favors certain actions over others.	Highlighted buttons, discolored text
Forced action	Any situation where the user needs to perform a certain action in order to proceed.	Required action (cannot be canceled)

In analysis, emphasis was on analyzing five main dark patterns, following described classification. Since several authors have done research based on these categories, they were chosen as a basis for evaluating the websites. Additionally, a similar taxonomy was followed by the OECD (2022), which further strengthened the reliance on these theoretical descriptions of the dark pattern.

Dark patterns are successful due to their reliance on human psychology, which involves common psychological tricks to compel users to take specific actions, such as the default effect, status quo, and framing (Jakobi and von Grafenstein, 2023). Related work on dark patterns has shown that interface interference and obstruction were the most common categories, while nagging was less frequently observed in news outlets (Soe et al., 2020). Although interface interference patterns and obstruction were present in the shopping category, Mathur et al. (2019) found that manipulations relying on language and emotional appeal were more common.

Similar work has been done by authors who manually evaluated the presence of dark patterns in websites (Mehrnezhad, 2020; Soe et al., 2020), as well as more recent initiatives that attempt to automatically detect dark patterns (Kirkman, Vaniea, and Woods, 2023). Recent work has focused on exploring the impact of different cookie consent designs on user decision making (Berens et al., 2024; Bielova et al., 2024), putting effort into developing bright patterns as a solution to exploit psychological tricks to the user's advantage.

2.2 Cookie consent

Due to the notice and choice mechanism present in cookie consents, the use of dark patterns is very popular among them (Habib et al., 2022). According to the GDPR, the term “consent” means any freely given, specific, informed, and unambiguous indication of a user’s desire (Alharbi et al., 2023). Some dark patterns can be considered as a violation of the GDPR, although many sophisticated patterns fall into the "gray" zone, i.e., are not expressly regulated. Research conducted shortly after the GDPR was introduced in 2019 showed that 99% of 300 websites with Scandinavian or English content didn’t allow users to refuse consent with a single click (Hu and Sastry, 2019). This violates the right of an individual to have the option to choose to refuse a cookie.

A significant increase in the number of cookies was found immediately after the introduction of GDPR, with 80% of the top 100 sites in the United Kingdom having implemented some form of cookie in 2019 (Hu and Sastry, 2019). A recent study from 2023 showed that the situation remains largely unchanged; in fact, looking at the global level, 50% of websites still do not have cookie consent, although the situation is better in European countries (Alharbi et al., 2023). In particular, one study discovered that websites outside of the EU

have less well-executed cookie design interfaces, giving consumers fewer options to make well-informed privacy decisions (Hu and Sastry, 2019). According to a survey of 3,947 respondents, users have developed a default cookie acceptance habit, which makes it even more important to offer a simple way to refuse consent (Bielova et al., 2024).

3 Methodology

3.1. Selection of website sample

As an initial sample, websites from the Tranco list (ID VQ2VN) were taken (Pochat et al., 2018). The Tranco list was chosen because it uses data from five different sources to appropriately rank the most popular websites. The website rankings were taken for a period of one month (from 03 May 2025 to 01 June 2025). An additional advantage of this list is that it only studies top-level domains, excluding their subdomains, which usually have the same cookie consent design. Also, it has been used in a large number of works, and it has an ID that can be used to easily track the list of web pages, which improves the research's reproducibility.

3.2. Identifying website categories

From the Tranco list, websites with the ".hr" domain were chosen, as this stands for Croatia's country code top-level domain. Since the term public sector websites includes a number of websites, the websites belonging to the public sector are identified first. Accordingly, websites were included in the analysis if they belonged to one of the three categories listed:

1) **Government bodies and administration websites** - this included government, ministries, agencies, offices, and counties
2) **Public institutions websites** - this included institutes, agencies, centers, universities, hospitals, and museums
3) **State-owned companies websites** - organizations that are majority owned by the state (e.g. post, transport, etc.)

3.3. Procedure

After the sample of websites was chosen, each website was analyzed to determine the presence of dark patterns. Prior to the analysis, a structured form was prepared to standardize the evaluation process. This form included information such as the website category, the presence of cookie banners, the position of the cookie banner, the number of options available to users, the applicable dark pattern categories, and other relevant characteristics. To ensure consistency in the website analysis process, the identification of dark pattern categories was guided by the examples and classification framework outlined in the theoretical section of this paper, based on the work of Gray et al. (2018).

Each website was manually reviewed by visiting its homepage from a web browser in private (incognito) mode. This approach was employed to ensure that prior browsing history or stored cookies would not affect the results of the analysis, such as the presence of cookie consent banners. A detailed checklist based on the standardized form with dark pattern categories and other observed characteristics was completed for each website. During the evaluation, cookie consent screens were taken so that they could be analyzed later and utilized to clarify particular dark patterns. Furthermore, in order to ensure that only legitimate public sector websites were included in the sample, each website was manually verified to confirm that it belonged to one of the following categories: government bodies and administration websites, public institutions websites, or state-owned companies websites.

4 Results

Following a detailed website selection procedure, 100 websites from the Tranco list were selected to provide a sample of Croatian public sector websites. The analysis revealed that 75% (75 out of 100) of the examined websites had a cookie consent interface, while the remaining 25% (25 out of 100) did not have any form of cookie consent implemented. The examination of dark patterns proceeded only with those websites that had implemented a cookie consent interface.

Out of the 75 websites that had cookie consent, 96% (72 of them) had some form of dark pattern, while 4% (3 of them) had no dark pattern present. Fig. 1 shows the overall frequency of dark pattern categories identified in cookie consent notices. The most frequently observed dark pattern categories were interface interference and obstruction, each identified on 28 websites, followed by forced action on 25 websites, and nagging, which appeared on 4 websites.

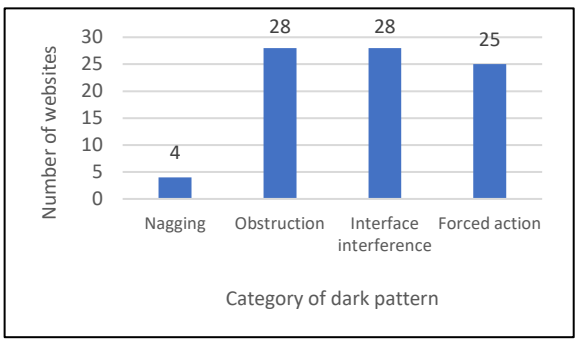

Figure 1. Frequency of dark pattern categories observed in cookie consent interfaces on Croatian public sector websites (N=75)

The interface interference category comprises four key subcategories: (1) aesthetic manipulation, (2) false hierarchy, (3) preselection, and (4) hidden information (Gray et al., 2018). Fig. 2 shows the distribution of specific subcategories within the interface interference category (N = 28), where aesthetic manipulation by colour was the most frequent subcategory (20 websites), to a lesser extent were represented false hierarchy (8 websites), hidden information (7 websites), and preselection (4 websites) subcategory.

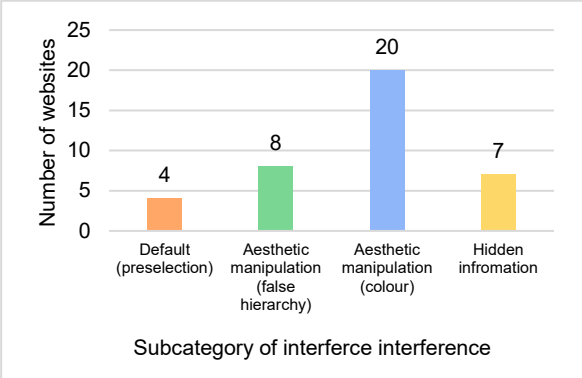

Figure 2. Frequency of interface interference subcategories observed in cookie consent interfaces on Croatian public sector websites (N =28)

4.1 Website Category

The analysis also examined the number of dark patterns present within each category of public sector websites. Fig. 3 illustrates the distribution of dark pattern categories across various types of public sector websites.

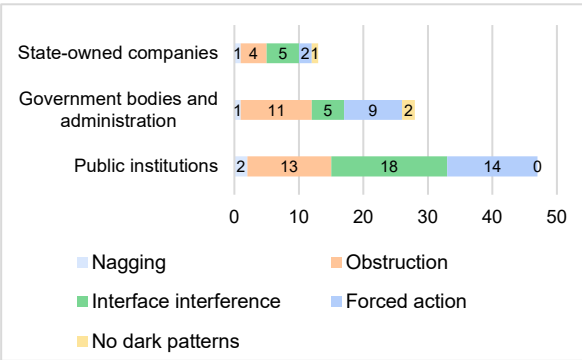

Figure 3. Frequency of dark pattern categories across different types of Croatian public sector websites (N = 75)

As shown in Fig. 3, nagging, forced action, interface interference, and obstruction were present in all three categories. The most frequent pattern in state-owned companies and public institution websites was interface interference, while obstruction was mostly present in government bodies and administration websites (in 11 examined websites).

4.2 Cookie Banner Position

The analysis also examined the positional placement of cookie banners on each website. Fig. 4 shows that cookie banners were predominantly positioned in the footer of the website (63 of them), less frequently in the middle (8 of them), and rarely in the header of the websites (4 of them). Additionally, several websites did not have any cookie banner implemented (25 of them).

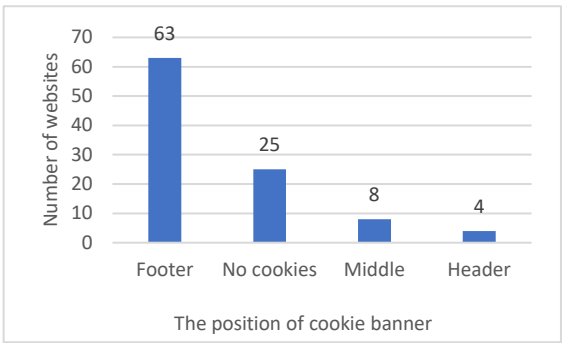

Figure 4. Frequency of cookie banner positions observed in Croatian public sector website (N=100)

4.3 Number of Options in Cookie Consent

To evaluate the extent of user autonomy in managing consent, the analysis examined the number of options available to users within cookie consent interfaces, on websites where cookies were present (N = 75). Fig. 5 shows that websites offering two options were the most prevalent (47%, 35 of them), these typically included options such as “Accept” and “Manage settings”, allowing limited user control. Furthermore, websites that provided only a single option were also represented (29%, 22 of them), most commonly through some variation of an "I agree", "Accept", or "Continue" button. Lastly, in a somewhat smaller proportion of cases (24%, 18 of them), three options were offered, typically including “Accept,” “Reject,” and “Customize” button, thereby allowing users greater control over their cookie preferences.

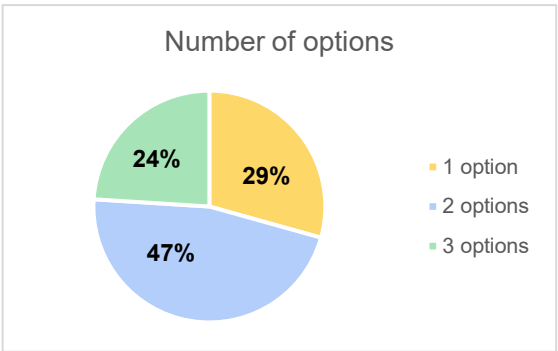

Figure 5. Number of options available to the users in cookie consent interfaces (N =75)

4.4 Number of Clicks to Reject Cookie

Finally, the number of clicks required to reject a cookie was analyzed. Fig. 6 shows that the majority of websites (74.67%, 56 websites) do not explicitly provide the option to reject cookies. Additionally, in 22.67% of cases (17 websites), users could refuse consent with a single click, while in 2.67% of cases (2 websites), rejecting cookies required two or more clicks.

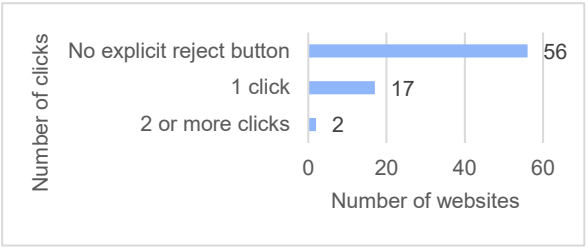

Figure 6. Number of user clicks required to reject cookie observed in cookie consent interfaces on Croatian public sector websites (N = 75)

4.5 Analysis of Dark Patterns Categories

As the categories of dark patterns are often intertwined and there is no clear distinction between them, this section details the criteria used to flag a website to a particular dark pattern. The description of each dark pattern was accompanied by a screen of the cookie consent to illustrate its representation in the listed dark pattern categories.

Nagging: The nagging category usually does not have a strict division; one most frequent forms are pop-ups that are hard to cancel. For example, before accepting cookie consent, a pop-up window appears asking whether the user wants to receive notifications about privacy policy updates, which the user must resolve in order to proceed. This was classified as a nagging pattern since the user's access to the page is interrupted by these options. Fig. 7 illustrates an example of a nagging pattern.

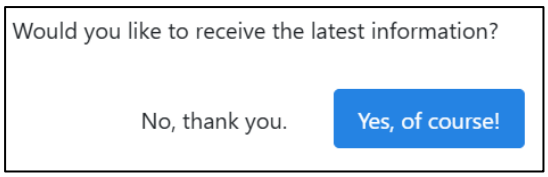

Figure 7. Example of a nagging pattern, a pop-up that interrupts the user's task

The second case, somewhat rarer, is the one in which the privacy settings are changed twice. First, cookie consent is accepted, and then immediately after that, another simpler form of cookie consent appears. This is classified as such a pattern because it burdens the user with an unnecessary number of interactions and information.

Obstruction: The obstruction category includes cases in which the process of accepting cookies must proceed in several steps in order to make it difficult to perform a certain action. In particular, this category included all cases of unequal path, for example, where in the initial view it was not possible to reject all cookies in one click, instead the user had to go to the privacy settings in order to change them. This was the main criterion for selecting cookie consent in this category, so it would not overlap with other dark patterns categories. Fig. 8 shows an example of an obstruction pattern where it is easier for the user to click on "I accept everything" button than go to the separate screen to change privacy settings.

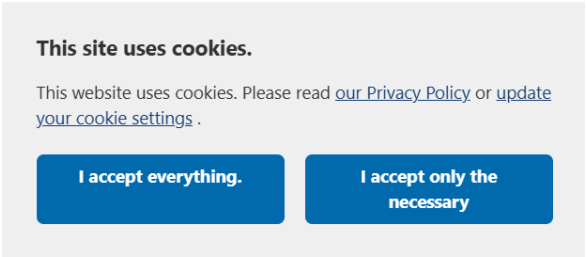

Figure 8. Example of obstruction pattern, only two options present

Interface interference: The interface interference was one of the main categories that included visual manipulations with the user interface that could affect the user's decision-making. Preselection is a common interface interference subcategory that is based on a default set or marked options that users usually accept in order to quickly perform an action. These subcategories included options in which checkboxes or other options were predefined, except for the strictly necessary cookies collection option. For example, the "I agree" checkbox can be previously selected for unnecessary cookies like marketing cookies, statistical cookies, and so on.

Fig. 9 shows an example of a preselection dark pattern where analytic cookies were selected by default.

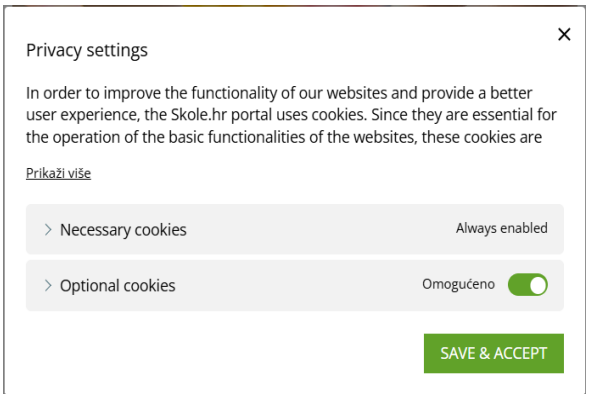

Figure 9. Example of preselection pattern, optional cookies marked by default

The second subcategory is aesthetic manipulation, which included options in which one button was visually emphasized relative to others, typically through the use of color. For example, when the accept button was prominently highlighted while the remaining options appeared grayed out. Furthermore, the false hierarchy subcategory comprised cases in which two buttons were highlighted, while the third option was weakly visible or expressed (e.g., the "Accept" and "Reject" buttons were highlighted, while the "Customize" option was weakly visible). The final subcategory, hidden information, encompassed options that were not easily visible, such as changing the privacy settings hidden within the text, displayed in a smaller font size, or displayed in the form of a link. Fig. 10 shows an example of interface interference subcategory named aesthetic manipulation by colour, where the "Allow" button is highlighted.

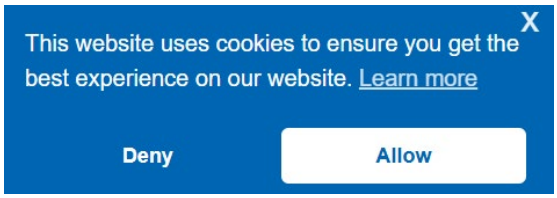

Figure 10. Example of aesthetic manipulation by colour

Fig. 11 shows a false hierarchy pattern where not all options are equally displayed (by size), and hidden information pattern in which the "Cookie settings" button is less noticeable.

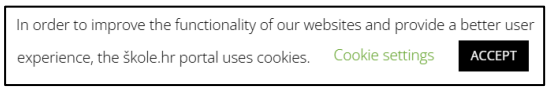

Figure 11. Example of false hierarchy and hidden information dark pattern

Forced action: The forced action category included cookie consent interfaces that compelled users to take action, or where users were forced to accept cookies due to a limited choice. A typical example of this option is where the user is only informed that cookies are being used, by accepting an option such as "I agree", "Continue", "Accept cookies", or "Close" button (Fig. 12).

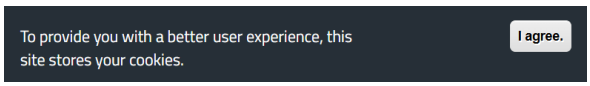

Figure 12. Example of forced action, only "I agree" button present

5 Discussion and Conclusion

In this research, a detailed analysis of 100 websites was carried out, with the aim of analyzing the presence of dark patterns in Croatian public sector websites. With regard to the first research question, the most common category of dark patterns observed was interface interference and obstruction patterns.

However, interface interference dark pattern was present due to its reliance on a strong psychological effect, and the large number of subtypes that fell into that category. Additionally, interface interference patterns were common in e-government websites, where dark patterns are often seen as highlighted buttons and preselected options (Alharbi et al., 2023). The European Commission (2022) study showed that preselection (as a subtype of interface interference) was the most popular dark pattern present in 41 out of 75 analyzed websites. However, the results present in this research show that the preselection pattern was not so common in public sector websites. This could be because personalization and data collection are less significant for public-sector websites than they are for commercial platforms such as shopping, news, or sports websites. For this reason, the preselection option was not predominantly used on public sector websites, as the goal was not to trick users into unknowingly accepting analytical or other optional cookies.

Regarding second research question, the number of options and clicks to refuse consent were examined separately. The most common cookie banner positions were located at the footer of the website. Previous research also shows that the footer and middle of a website are the most common places where cookies are placed (Mehrnezhad, 2020; Soe et al., 2020). Although it cannot be stated with certainty, the footer is generally a suitable place for cookie consent interfaces, as it often receives more user interaction (Utz et al., 2019).

Research conducted after GDPR was introduced revealed that certain cookie consent did not allow users to refuse consent with a single click (Hu and Sastry, 2019). As can be seen from the results of research conducted in this paper, this number has not improved significantly. This is concerning because the large number of websites makes it difficult for the user to find options for rejecting cookies. It is recommended that future regulations mandate an explicitly visible option for rejecting cookies.

The contribution of this work is evident in the dark patterns analysis on public sector websites that have not received sufficient attention in the literature. Thus, this addresses the gap in understanding what dark patterns are present on public sector websites and further areas for improvement. It has also been observed that a large number of sites do not have cookie consent, which is acceptable only in cases when they do not collect any data about users.

The limitations of this work refer to the fact that only a small sample of popular public sector websites was analyzed, to gain a more comprehensive understanding, the research should be repeated using a larger sample. In addition, the classification of dark patterns itself is rather vague, and there are no strictly defined rules about what belongs to which dark pattern category. For this reason, comparisons should be taken

with caution, because the very process of determining whether something belongs to the dark pattern category is quite subject to the researcher's assessment. Future research should focus on defining criteria, such as a checklist with detailed sub-criteria for categorizing different types of dark patterns. This would facilitate more objective assessments and allow for easier comparison of results across studies. Usable privacy research frequently includes experiments on a specific prototype or scenario to better understand the user's thinking and the impact of dark patterns (Fischer-Hübner and Karegar, 2024). Therefore, deeper research and analysis of the human aspect of privacy and security should be conducted. In addition to the future initiatives, apart from the dark pattern analysis itself, strengthening bright pattern practices should be considered to reduce this gap.

The specific implications of the research suggest that efforts should be made to minimize the appearance of interface interference and obstruction patterns, as they were observed in the majority of cases. Some of these practices include placing buttons in the same sizes and colours, as well as ensuring sufficient visibility of all options. Despite the psychological aspect of these patterns, mitigating their impact can be achieved by educating users and increasing their awareness of the good and bad cookie design practices.

Recommendations for future institutional practices can be proposed for each website category to promote ethical interface design. State-owned companies and public institutions should focus on mitigating interface interference patterns by avoiding deceptive visual manipulations and ensuring a neutral design that enables transparent user choices. Government bodies and administration websites should primarily address obstruction patterns by implementing a cookie consent interface design that minimizes the number of actions required for users to reject cookie consent. Since public sector websites serve a large audience, a general recommendation for all categories is to provide users with simple and clear options to withdraw consent. Implementing these practices is essential to strengthen the citizens' trust in public sector websites.

References

Alharbi, J. A., Albesher, A. S., & Wahsheh, H. A. (2023). An Empirical Analysis of E-Governments' Cookie Interfaces in 50 Countries. *Sustainability (Switzerland)*, *15*(2). doi:10.3390/su15021231

Berens, B. M., Bohlender, M., Dietmann, H., Krisam, C., Kulyk, O., & Volkamer, M. (2024). Cookie disclaimers: Dark patterns and lack of transparency. *Computers & Security*, *136*, 103507. doi:10.1016/j.cose.2023.103507

Bielova, N., Litvine, L., Nguyen, A., Chammat, M., Toubiana, V., & Hary, E. (2024). The effect of design patterns on (present and future) cookie consent decisions. In *33rd USENIX Security Symposium (USENIX Security 24)* (pp. 2813-2830).

Brignull, H., Leiser, M., Santos, C., & Doshi, K. (2023, April 25). *Deceptive patterns – user interfaces designed to trick you.* Retrieved December 19, 2024, from http://darkpatterns.org/

Distler, V., Fassl, M., Habib, H., Krombholz, K., Lenzini, G., Lallemand, C., Cranor, L. F., & Koenig, V. (2021). A Systematic Literature Review of Empirical Methods and Risk Representation in Usable Privacy and Security Research. In *ACM Transactions on Computer-Human Interaction* (Vol. 28, Issue 6). Association for Computing Machinery. doi:10.1145/3469845

European Commission: Directorate-General for Justice and Consumers, Lupiáñez-Villanueva, F., Boluda, A., Bogliacino, F., Liva, G., Lechardoy, L., & Rodríguez de las Heras Ballell, T. (2022). *Behavioural study on unfair commercial practices in the digital environment : dark patterns and manipulative personalisation : final report*, Publications Office of the European Union. doi: 10.2838/859030

Fischer-Hübner, S., & Karegar, F. (2024). Overview of Usable Privacy Research: Major Themes and Research Directions. *The Curious Case of Usable Privacy: Challenges, Solutions, and Prospects*, 43-102. doi:10.1007/978-3-031-54158-2_3

Gartner (2024). *Gartner 2024 Hype Cycle for Emerging Technologies Highlights Developer Productivity, Total Experience, AI and Security*. Retrieved December 19, 2024, from https://www.gartner.com/en/newsroom/press-releases/2024-08-21-gartner-2024-hype-cycle-for-emerging-technologies-highlights-developer-productivity-total-experience-ai-and-security

Gray, C. M., Kou, Y., Battles, B., Hoggatt, J., & Toombs, A. L. (2018). The dark (patterns) side of UX design. In *Conference on Human Factors in Computing Systems - Proceedings*, *2018-April*. doi: 10.1145/3173574.3174108

Habib, H., Li, M., Young, E., & Cranor, L. (2022, April 29). "Okay, whatever": An Evaluation of Cookie Consent Interfaces. In *Conference on Human Factors in Computing Systems - Proceedings*. doi: 10.1145/3491102.3501985

Hu, X., & Sastry, N. (2019, June). Characterising third party cookie usage in the EU after GDPR. In *Proceedings of the 10th ACM Conference on Web Science* (pp. 137-141). doi: 10.1145/3292522.3326039

ICPEN (2024). *ICPEN Sweep finds majority of websites and mobile apps use dark patterns in the marketing of subscription services*. Retrieved December 19, 2024, from https://icpen.org/news/1360#_ftnref1

Jakobi, T., & von Grafenstein, M. (2023). What HCI Can Do for (Data Protection) Law—Beyond Design. In *Human Factors in Privacy Research,* pp. 115 - 136. doi:10.1007/978-3-031-28643-8_6

Kirkman, D., Vaniea, K., & Woods, D. W. (2023). DarkDialogs: Automated detection of 10 dark patterns on cookie dialogs. In *Proceedings - 8th IEEE European Symposium on Security and Privacy, Euro S and P 2023*, 847–867. doi: 10.1109/EuroSP57164.2023.00055

Kitkowska, A. (2023). The hows and whys of dark patterns: Categorizations and privacy. In *Human Factors in Privacy Research*, 173-198. doi: 10.1007/978-3-031-28643-8_9

Mathur, A., Acar, G., Friedman, M. J., Lucherini, E., Mayer, J., Chetty, M., & Narayanan, A. (2019). Dark patterns at scale: Findings from a crawl of 11K shopping websites. In *Proceedings of the ACM on Human-Computer Interaction* (Vol. 3, Issue CSCW). Association for Computing Machinery. doi:10.1145/3359183

Mehrnezhad, M. (2020). A Cross-Platform Evaluation of Privacy Notices and Tracking Practices. In *Proceedings - 5th IEEE European Symposium on Security and Privacy Workshops, Euro S and PW 2020*, 97–106. doi: 10.1109/EuroSPW51379.2020.00023

Organisation for Economic Co-operation and Development (2022). Dark commercial patterns. *OECD Digital Economy Papers*. No. 336. OECD Publishing Paris. doi: 10.1787/44f5e846-en

Pochat, V. L., Van Goethem, T., Tajalizadehkhoob, S., Korczyński, M., & Joosen, W. (2018). Tranco: A research-oriented top sites ranking hardened against manipulation. In *Proceedings of the 26th Annual Network and Distributed System Security Symposium* (NDSS 2019). doi: 10.14722/ndss.2019.23386

Soe, T. H., Nordberg, O. E., Guribye, F., & Slavkovik, M. (2020, October). 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* (pp. 1-12). doi:10.1145/3419249.3420132

Sørensen, J., & Kosta, S. (2019, May). Before and after GDPR: The changes in third party presence at public and private european websites. In *The World Wide Web Conference* (pp. 1590-1600). doi: 10.1145/3308558.3313524

Utz, C., Degeling, M., Fahl, S., Schaub, F., & Holz, T. (2019, November). (Un) informed consent: Studying GDPR consent notices in the field. In *Proceedings of the 2019 ACM SIGSAC conference on computer and communications security* (pp. 973-990). doi:10.1145/3319535.3354212