/ЧЛАНЦИ

UDC 366.626; 004.738.5:339

CERIF: S 110

DOI: 10.51204/Anali_PFBU_24101A

Mateja DUROVIC, PhD*

HOW TO PROTECT CONSUMERS IN THE DIGITAL ERA: AN EXAMPLE OF THE ONLINE CHOICE ARCHITECTURE

The ongoing process of digitalisation has brought a number of new challenges to the existing regulatory frameworks for consumer protection. One of these major challenges is the phenomenon of the online choice architecture, which is used to push consumers to make specific economic decisions while acting as participants of the digital market. In the majority of cases, such pressures should not be allowed as they rely on consumers' vulnerability. This paper examines the phenomenon of online choice architecture and the fact that the existing consumer law framework does not provide adequate legal protection to the consumers from online choice architecture, calling for a consumer law reform that would enable better protection of consumers.

Key words: *Consumer law. – Online choice architecture. – Digital Services Act. – Unfair Commercial Practices Directive. – Dark patterns.*

* Full Professor of Law, King's College London, United Kingdom, *mateja.durovic@kcl.ac.uk*.

1. INTRODUCTION

In the contemporary digital world, online choice architecture represents a particular challenge for consumer protection. Discussions surrounding online choice architecture (OCA), or dark patterns, typically centre on the negative consequences of the defaults, the difficulty of obtaining consent, or the ways in which data is being exploited to capitalise on consumer unawareness. This paper argues that OCA and the use of defaults demand the extension of the category of vulnerable consumers to include all users in an online environment in which dark patterns can be detected. To illustrate the vulnerability of consumers, this contribution will look at fertility apps as a particularly sensitive case study, following the research conducted by Katherine Kemp (Kemp 2023, 1–33).

In this paper, we will also present personal data as a modern currency when it comes to digital consent. The hope is that this will raise awareness and show that although providing personal data seemingly comes at no cost to consumers, it is the price paid for the use of any service in the online environment, being revenue-generating for businesses. This is paradoxical as, although price is one of the most important factors when it comes to the consumers' decision-making framework, data privacy is often neglected despite it directly influencing consumers (Durovic, Lech 2021, 702). The idea of data as a currency is later explored in the fifth section of the paper. Analogy demands the inclusion of consumers active in online environments where OCA contains dark patterns into the category of vulnerable consumers based on their inability to compare services in regard to the main currency of the online world: data (Esposito, Grochowski 2022, 26).

The first section of the paper delves into three prevalent taxonomies employed in the surveyed literature. After explaining the terminology used in the sector and later employed in the paper, one of the taxonomies is chosen for the purpose of consistency. Throughout the second, third and fourth sections, the concepts of defaults, consent and data are explored and the connections between them are explicated. These sections bridge the gap in the current literature and explore the most prevalent issue that appears in data processing, namely obtaining informed consent. It will be shown how defaults work to obtain an uninformed form of consent, which is then used for the collection and processing of data, and which consumers are unaware of. The sixth section explores five solutions identified in the literature that seem to tackle the problem of obtaining informed consent. After these are analysed, two personal solutions are proposed and explored, before a summary of the paper is provided.

2. ONLINE CHOICE ARCHITECTURE

Online choice architecture is an umbrella term that refers to the environment created by marketers and content designers, alongside user experience and interaction designers (CMA 2022b, 2). OCA can be used to hide dark patterns that aim at influencing consumer behaviour. Through detailed literature research, it has been observed that multiple taxonomies have been used to describe and organise these dark patterns. For completeness purposes, three such taxonomies will be summarised, before choosing one of them and justifying the choice.

Gray *et al.* (2018, 1) discusses five types of dark patterns: nagging, obstruction, sneaking, interface interfering, and forced action. Nagging is described as a diversion from the current task that can occur multiple times. Obstruction refers to acts that block the task flow, increasing the difficulty of performing it; methods of achieving this include introducing intermediate currencies, making it more difficult to compare prices of services, a practice known as price comparison prevention, or requiring users to sign up for an account that is almost impossible to close, aka 'roach motel'. Sneaking refers to practices aimed at disguising relevant information; such practices include actions that do not lead to the perceived result, aka 'bait and switch', hidden costs, sneaking items into the basket, and forced continuity of different subscriptions. Interface interfering refers to attempts to create a bias in favour of certain aspects existent within the user interface, with identified tactics including hiding information, preselecting the unfavourable options, or manipulating the user interface.

These manipulations may amount to: adding false countdowns to influence consumers into deciding quicker, making an option appear more prevalent, including disguised ads that assume the form of interactive games or answering trick questions. Forced action refers to the necessity to take additional steps to advance towards the desired outcome. Such actions may involve sharing additional data, obtaining additional benefits for adding more friends or completing tasks to obtain something available for purchase.

In the United Kingdom, the Competition and Markets Authority (CMA) used another taxonomy, proposing that dark patterns be divided into three components: choice structure, choice information, and choice pressure. Choice structure refers to how the options are presented. The altering of the method of presenting information comprises the choice information component. Lastly, choice pressure considers practices that aim to influence the consumer's decision-making. The relevant OCA practices identified by the CMA are encompassed in Table 1 (CMA 2022, v).

Table 1. OSA practices according to component

Choice Structure	Choice Information	Choice Pressure
Defaults Ranking Partitioned pricing Bundling Choice overload and decoys Sensory manipulation Sludge Dark nudge Virtual currencies in gaming Forced outcomes	Drip pricing Reference pricing Framing Complex language Information overload	Scarcity and popularity claims Prompts and reminders Messengers Commitment Feedback Personalisation

Source: CMA 2022a, v.

Another taxonomy is the one structured by Mathur *et al.* (2019, 81:5). This taxonomy lists five dimensions that help us to characterise each dark pattern, rather than naming the different practices, as previous taxonomies do. The five dimensions are: asymmetric, covert, deceptive, hides information, and restrictive. An asymmetric dark pattern enhances certain elements of the interface to the disadvantage of others. A dark pattern is covert if it hides information from users through the design of the interface aimed at influencing their choices. A deceptive dark pattern induces false beliefs through misleading statements or omissions, even if they are affirmative. To qualify for the 'hides information' dimension, a dark pattern must delay making necessary information available to the user. A restrictive dark pattern restricts the choices that are available to the user (Mathur *et al.* 2019, 81:6).

It is submitted that the confusing nature of this taxonomy deems it worthy of rejection. It must be observed that the 'covert' and 'hides information' dimensions appear to overlap considerably. This makes it harder to accurately characterise and classify dark patterns. Further clarification, describing the differences between the dimensions highlighted above, is necessary before this taxonomy can be used for the purposes for which it was instituted, namely, to characterise and classify dark patterns.

3. DEFAULTS

Despite the comprehensive presentation provided above, the paper focuses on defaults, and at times dark nudges, information overload and framing. Within the following contribution, dark nudges and nudges will be used to convey the same meaning, referring to practices that are meant to influence consumers and ensure that they reach a desired outcome. For the purpose of clarity, in the following contribution, 'default' will be used to highlight that a consumer cannot reject the terms and conditions if they are unhappy with the privacy policies, equally they are unable to negotiate or modify privacy policies.

A default can be considered a pre-selected option when consumers are faced with a particular action or set of options. Defaults can have both a positive and a negative impact on the consumers' ability to follow their interests. For example, a pre-installed anti-virus could help consumers to avoid computer viruses. However, this can also mean that consumers are enrolled in a subscription that forces them to pay for something they may not need (CMA 2022b, 2). Additionally, this also prevents the consumers from conducting their own research on what is available on the market and choosing the option that fits them best, impacting competition. Furthermore, it has been pointed out by the CMA that such conduct may also increase a business's market share beyond what the product is worth (CMA 2022b, 30). Hence, businesses may be discouraged from competing with one another to provide better offers and attract customers and focus on creating partnerships that promote bundling.

Defaults are problematic when they entertain and rely on consumer biases. Consumers tend to act quicker, and their attention spans are shorter. In addition, consumers skim rather than read the information presented and are more responsive to recommendations (Duggan, Payne 2011, 3). Weinreich *et al.* showed that out of the pages surveyed, 25% had been displayed for less than 4 seconds, 52% of the visits lasted less than 10 seconds, with only 10% of visits lasting longer than 2 minutes (Duggan, Payne 2011, 4). By exploiting this modified online behaviour, defaults exert a strong effect on consumer behaviour. Jachimowicz *et al.* (2019, 161) showed that a default is 27% more likely to be selected out of two options. Additionally, opt-out defaults have been proven to lead to a greater uptake of the pre-selected decision. An old famous study by Eric Johnson and Daniel Goldstein surveyed the prevalence of organ donors in countries with an opt-in and an opt-out system for organ donation. It has been highlighted that approximately 90% of the individuals

are organ donors when opt-out defaults are employed, while only 10% of the individuals will donate organs when the system is based on opt-in defaults (Johnson, Goldstein 2003, 1338).

The practice of taking advantage of the benefits of opt-out defaults is most prevalent when businesses try to collect data that can later be treated as a business asset. For example, the Clue app, a mobile application tracking fertility, automatically uses customer data for research purposes, provided that the terms have been accepted. There is an option to opt-out of this, by contacting the company.[1] Hence, the cost of opting-out and protecting personal data is increased through the use of defaults.

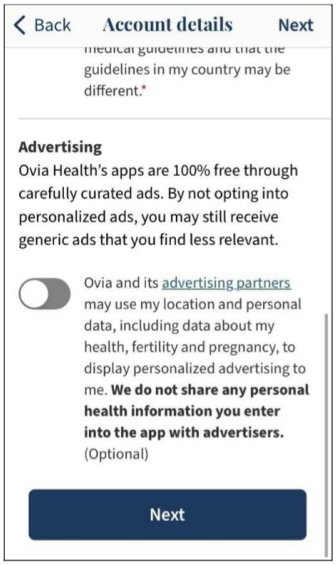
4. CONSENTING IS THE NEW DEFAULT

Choice architects are the ones that decide how information will be conveyed to consumers, what are the actions that consumers need to take, and what the options will look like, including what is the default. It is evident that the information can be thus framed to highlight certain aspects over others, which will remain undetected provided the consumer embodies the online behaviour described above. Therefore, choice architects have the power of influencing how defaults are presented, in order to take advantage of behavioural economics when obtaining the consumer's consent.

This practice can be observed in the choices presented in the Ovia app regarding data sharing. The OCA has been designed to create the impression that there is no possibility that the consumers' personal health information will be shared with advertisers. This has been done through the use of bold lettering right next to the 'Next' button. However, the sentence prior to the bold lettering explicitly mentions that personal health data may be shared with advertisers to display more personalised data. These sentences are contradictory as information regarding health, fertility and pregnancy qualifies as personal health information. After reading this the consumer may still be conflicted about whether or not to opt-in to this section. The first paragraph of the setting description is used to eliminate such uncertainty. The use of the construction 'you may still receive generic ads that you find less relevant' is meant to present opting-in as a recommendation that will bring numerous benefits to the consumer.

[1] Clue Privacy Policy, *https://helloclue.com/privacy*, last visited March 11, 2024.

Figure 1. Screenshot of the Ovia app account settings



Source: Kemp 2023, 15.

It can be noted how the consumers' ability to compare the conditions under which products or services are offered is reduced by manipulating key pieces of information and choosing which characteristics will be displayed first or written in bold. The inability to compare such conditions is a key point in our discussion as without the ability to understand which providers better safeguard their private data; consumers cannot make this a criterion in their choice, ultimately vitiating the consumer's consent. Businesses lack an incentive to compete in the domain of safeguarding consumer data or offering autonomy over how the data is used. This can be noted in the study conducted by Katherine Kemp, where one third of the apps analysed state in the fine print of their privacy policies that consumer data may be sold as a business asset, despite previously assuring consumers that they do not sell data or they never sell data (Kemp 2023, 13).

5. DATA

This section takes a look at the current regulation for obtaining consent for data processing purposes. It will be shown that data may be processed, provided that prior consent is obtained from the consumer. Customarily, the purposes for which the data is processed are laid out in the privacy policy.

This allows companies to sneak in additional purposes and obtain the consumer's consent through the default acceptance of the conditions, which is required prior to completing certain actions.

Although under data privacy law consent is required for data processing, it is unlikely that consent is given freely, due to the complex nature of framing the request. Under Article 7 of the General Data Privacy Regulation (GDPR), a request for consent 'shall be presented in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language'.

The average time necessary to read privacy policies is very long. Coupled with the shorter attention spans of users, this allows businesses to sneak in multiple processing purposes that allow them to handle the data in ways that consumers may have not wanted. The requirement imposed by the GDPR fails to ensure that consumers understand the nature of the request. The current environment permits the abuse of behavioural patterns, with the aim of hiding the purposes for which data is used and obtaining consent for multiple purposes. Sanchez-Rola *et al.* (2019, 340) shows that despite the GDPR, tracking may take place without the user's consent. The study shows that 90% of websites create cookies prior to the consumers deciding whether or not they want to be tracked.

Even more concerning is the fat that although consumers agree to share their data, they do not understand what data will be collected. There may be a false impression that the collection of data takes place when signing up. However, the data collection takes place at multiple levels, from inputted data to inferences drawn from the news articles accessed or the use of other features provided within an app. The Ovia app provides a health assessment meant to provide a more tailored experience to users. However, this is another opportunity to create a virtual profile for the user, which can later be sold to advertisers or other companies. Examples of the questions have been procured by Katherine Kemp can be seen below.

Box 1. Examples of Ovia Health Assessment questions

Box 1 – Examples of Ovia "Health Assessment" Questions

"How many pregnancies have you had?

"How many pregnancy losses (miscarriages) have you had?"

"Check the box if you have a history of: Endometriosis; PCOS; Uterine Fibroids; Diagnosed infertility; Multiple anormal paps; Depression; None of the above"

"Do you have a history of malignancy (cancer)?"

"Do you have painful periods?"

"Do you have a uterus?"

"In the last 12 months, did you ever eat less than you felt you should because there wasn't enough money for food?"

"Are you worried that in the next 2 months, you may not have stable housing?"

"How often does this describe you? I don't have enough money to pay my bills: Never; Rarely; Sometimes; Often; Always"

"In the last 12 months, have you ever had to go without health care because you didn't have a way to get there?"

"Are you afraid you might be hurt in your apartment building or house?"

"What is your highest education level?"

Source: Kemp 2023, 7.

Under the current regime, the nature of procuring consent is a paradox. Consenting to an action would imply that there is an alternative. However, the reality is that most often the alternative to giving consent is accepting that the consumer will not obtain the product or service. Hence, it can hardly be argued that one can even talk about obtaining consent for data processing in a world where the processing of data conditions the consumer's access to services. Therefore, obtaining consent appears to be just a façade.

Moreover, the inability to understand or monitor how data is used or how it is collected further supports the inclusion of online users in the category of vulnerable consumers in cases where OCA relies on dark patterns. The fertility apps privacy terms describe the collection of technical data. Consenting to the general terms and to the collection of this data allow the app to share the data collected from consumers with partners. For example, the Flo app shares data with AppsFlyer which later shares with its partners, including Pinterest, Google Ads, Apple Search Adds, and Facebook (Kemp 2023, 17).

6. PERSONAL DATA: A NEW CURRENCY SHAPING CONSUMER BEHAVIOUR

When choosing different products or services, price is often the most important factor guiding the consumer's decision. In the online environment, most services appear to be free, but disclosing personal data is the price paid by consumers. A logical conclusion would be that data privacy should replace price as a comparison criterion when using online services. In turn, businesses would have to compete to improve their data policies to attract consumers. As previously discussed, consumers do not spend time reading privacy policies as they perceive using online services as free, despite being concerned about having control over their personal data.

Personal data acts as an intermediary or a virtual currency that is interposed between consumers and their enjoyment of the online environment. The recent EU Enforcement and Modernisation Directive[2] ensure that consumer protection law safeguards consumers even in such cases where services or products are obtained in exchange of the provision of data.[3] A similar mention is made within the European Digital Content Directive.[4] This neglected currency facilitates the reluctance of businesses to change their data policies without regulatory intervention. Coupled with the absence of competition between businesses retarding making their services available at a lower 'data cost' for consumers, this supports the lack of meaningful alternatives when choosing whether to consent to the data policies. Absent such meaningful alternatives, accepting privacy policies or terms and conditions has become akin to a default due to several factors. First, it is the take-it-or-leave-it nature of these agreements that makes it impossible for consumers to have autonomy over their data. Second, the erroneous belief that the default 'I agree' is a recommendation made by choice architects (Sanchez-Rola 2019, 344) contributes to consumers blindly agreeing to the terms. For the purpose of this contribution, the opt-out agreements, where pre-selected options are available, are taken as a form of

[2] Directive (EU) 2019/2161 of 27 November 2019 amending Council Directive 93/13/EEC and Directives 98/6/EC, 2005/29/EC and 2011/83/EU of the European Parliament and of the Council as regards the better enforcement and modernisation of Union consumer protection rules [2019] *OJ L* 328/7.

[3] *Ibid*., 31.

[4] Directive (EC) 2019/770 of 20 May 2019 on certain aspects concerning contracts for the supply of digital content and digital services [2019] *OJ L* 136/1, recital 24.

a default 'I agree'. Third, there is another erroneous belief that as accepting is the default and many other consumers had previously accepted the same terms and conditions, these cannot be 'that harmful'.

These factors facilitate the manipulation of consumers by businesses. For example, the My Calendar fertility app assures consumers that it will never sell their data. However, in its privacy policy, it states that 'If we are involved in a merger, acquisition, reorganization, restructuring, or other sale or transfer of all or any portion of our assets or business, that could involve your Personal Information and User Data being transferred to the buyer or surviving entity' (Kemp 2023, 13). This may seem harmless at first glance, but it allows the app to treat the user's data as a business asset and later share it with partners.

Another subscription-based app, Pregnancy+, provides two levels of services for its members, the gold and silver standard. Both involve tracking the consumer's data with the aim of delivering the best personalised experience. The app looks at what functions the consumer uses more and how they access it. For the gold members, the app uses the consumers' advertising ID. Despite allowing Phillips to show consumers targeted advertisements through external advertising channels, using the identifier allows Google to independently use the advertising ID to personalise the advertisements gold members will be shown in the Google app (Kemp 2023, 17).

The ability to access personalised content does not seem to be detrimental to the consumers' enjoyment of the online environment. However, their inability to have autonomy over their own data surely is. As explored above, the language used in privacy policies hides how and what data will be collected. Often the ambiguity of the OCA also manages to convince consumers to share their data. It is argued that the absence of the ability to understand the above-mentioned, coupled with the effect and use of defaults, calls for the scope of the 'vulnerable consumer' category to extend to encompass all the users of online environments where dark patterns are present. Typically, vulnerable consumers include the elderly and the young, due to their unfamiliarity with the online environment. However, extension is motivated by the inability to provide informed consent of the aforementioned users. In addition, the consumers often share sensitive data, as is the case of the consumers that use the services provided by the above-analysed applications. The issue here is that such data will be used to target consumers while they are using other online services. Such targeting may contribute to additional distress to consumers. It is argued that the lack of autonomy characteristic to online environments, where the OCA is dominated by dark patterns, calls for the inclusion of consumers present in the aforementioned environment in the category of vulnerable consumers.

7. LEGAL SOLUTIONS

Various solutions aimed at ensuring that defaults or the OCA do not vitiate consent have been implemented in various jurisdictions. In the United Kingdom, the Competition and Markets Authority (CMA) proposed two solutions to counteract the negative effects of defaults and dark patterns in the context of OCA and to ensure that informed consent is obtained. First, the CMA put forward the necessity for a mandatory default that is in the interest of the consumer (CMA 2022a, 39) but that this solution would not be effective for the following reasons. Determining what is in the best interest of each consumer is impossible as each consumer is different. Hence, further guidance is necessary for the implementation of the mandatory default. In addition, there are important issues that still need to be addressed before this solution can be adequately considered. Would the authorities rely on the benchmark of the average consumer when determining what the mandatory default would be? The average consumer is a legislative construct implying that each consumer is an individual who is reasonably well-informed, observant, and circumspect (Keller *et al.* 2011, 379).[5] How would the authority ensure that businesses comply with this requirement and that the default they propose is the one that is the closest to the interest of the consumer, rather than the most business-wise one?

Some may argue that Jachimowicz *et al.* (2019, 162) answers these challenges by proposing the smart default. These are defaults that use behavioural economics to deliver a tailored pre-selected option that is in the interest of each particular consumer. The aim is to produce the perfect default for each consumer, to avoid situations in which defaults nudge consumers into choosing less favourable options. Furthermore, smart defaults would eliminate the potential of a blanket approach which otherwise fails to satisfy all the consumer's preferences.

However, it is submitted that this solution needs to withstand different challenges as it will require the collection and processing of data. It is considered that smart defaults are in no way more advantageous than traditional defaults, due to the lack of transparency that they seem to feature and the processes that they are derived from. Thus, it is impossible to ascertain whether a smart default would be the option that best caters to the interest of the consumer, based on the collected data, and is not influenced by the interests of various business entities. In addition, it is necessary to obtain consent for the processing of data. This would be problematic as it

[5] Consumer Rights Act 2015, s 64(5).

will run into difficulties outlining characterising consent and ensuring that consent is informed and given freely. If consumers do not understand how their data will be used and are unaware of all the conditions they agree to, then it cannot be argued that consent is 'freely given, specific, informed'. It is submitted that more guidelines would be provided regarding what qualifies as 'plain and intelligible language'.

Second, the CMA proposed that businesses should be required to ensure that consumers make an active choice (CMA 2022a, 44). This solution seems to answer the challenge of a lack of alternative choices, other than agreeing to a privacy policy or to the terms and conditions. However, there is at least one challenge that this solution cannot answer, namely its inability to ensure that it is resistant to the influence of dark patterns, such as dark nudges. It must be considered that, although having alternative choices seems to improve competition in terms of data privacy and, consequently, incentivises businesses to provide better privacy policies; businesses may still take advantage of behavioural economics through OCA, to the detriment of the consumers.

However, from the European Union perspective, it is also important to take into consideration the powerful Directive 2005/29/EC on unfair commercial practices (UCPD).[6] The UCPD covers unfair practices in general, and thus, while the online choice architecture or the term 'dark pattern' may not have a legal definition in the UCPD, most instances of dark patterns are considered unfair commercial practices and can be covered by the scope of the UCPD (Hacker 2021). Further, the European Commission has issued guidance regarding the interpretation and application of the UCPD with regards to dark patterns, including a section explaining how the relevant provisions of the UCPD can be used to challenge the fairness of practices when dark patterns are involved, in the context of business-to-consumer commercial relationships (European Commission 2021, 4.2.7).

The UCPD protects consumers against misleading practices and misleading omissions that deceive or are likely to deceive the average consumer.[7] Recognizably, in many instances of dark patterns, 'relevant information is hidden or provided in a way that makes the consumer take a certain

[6] Directive 2005/29/EC of the European Parliament and of the Council of 11 May 2005 concerning unfair business-to-consumer commercial practices in the internal market, amending Council Directive 84/450/EEC, Directives 97/7/EC, 98/27/EC and 2002/65/EC of the European Parliament and of the Council and Regulation (EC) No 2006/2004 of the European Parliament and of the Council ('unfair commercial practices directive'), *OJ L* 149/28.

[7] Articles 6 and 7 UCPD.

decision which, in absence of that specific practice, they otherwise would not have taken' (BEUC 2022, 7). More significantly, however, a commercial practice will be considered misleading as long as it 'in any way, including overall presentation, deceives or is likely to deceive the average consumer, even if the information is factually correct'.[8] The emphasis on 'overall presentation' here is fundamental in regulating dark patterns. Often, online users are manipulated by dark patterns that do not relate to any truth-apt information or content. For example, in the case of sensory manipulation where one option is made to appear more colourful and visually striking while the other option is purposely designed to be dull and less noticeable, there is no material information present that can be proven true or false to begin with. In such cases the manipulative factor is solely to do with the deceptive presentation of the choices to users.

The European Commission has also issued guidelines regarding non-fact-based manipulative practices, such as visually obscuring important information or promoting a specific option, using trick questions and ambiguous language, or deploying default interface settings, e.g. using pre-ticked boxes, inter alia. While it could be argued that the use of the term 'overall presentation' is overly broad and inherently vague, Article 6(1) of the UCPD does contain a list of elements to be considered in the assessment of unfairness. Notably, Article 6(1) (d) refers to 'the price or the manner in which the price is calculated', which has strong relevance for many types of dark patterns, such as drip pricing. That said, this list of elements clearly lacks scope in the context of online business-to-consumer transactions, and there is an opportunity to expand it to more easily apply to dark patterns.

Articles 8 and 9 of the UCPD regulate aggressive practices, which also has a strong impact on the digital market (Kaprou 2022, 77). Accordingly, a commercial practice 'shall be regarded as aggressive if, in its factual context, taking account of all its features and circumstances, by harassment, coercion, including the use of physical force, or undue influence, it significantly impairs or is likely to significantly impair the average consumer's freedom of choice or conduct with regard to the product and thereby causes him or is likely to cause him to take a transactional decision that he would not have taken otherwise'.[9]

8 Article 6 UCPD.

9 Article 8 UCPD.

Moreover, the UCPD also provides the material elements to consider when assessing an aggressive practice, including the 'exploitation by the trader of any specific misfortune or circumstance of such gravity as to impair the consumer's judgement, of which the trader is aware, to influence the consumer's decision with regard to the product'.[10]

This provision can successfully capture many forms of dark patterns if 'the trader, via the techniques used to revamp the user interface (e.g., A/B testing), is aware of the choices that are most likely to be made by consumers under different circumstances and therefore can use that fact to their own advantage' (BEUC 2022, 8). Having said that, practical difficulties may arise during investigation and enforcement, since relying on this provision involves demonstrating, as a matter of fact, that the trader possesses such knowledge. This can be a difficult burden of proof to satisfy.

The European Union has also recently adopted the new Digital Services Act (DSA)[11] which partially addresses OCA. The Digital Services Act aims at regulating OCA, to prohibit nudging techniques or other dark patterns that would prevent consumers from making free choices or interacting with the platform. Besides the solution proposed by the Digital Markets Act,[12] which so far seems the only viable one, two other solutions may be worthy of consideration. First, it may be useful to show consumers the sum generated by companies from their data. A study conducted amongst 600,000 US households showed that households that regularly received a letter comparing their own energy consumption to that of similar neighbours reduced their consumption by an average of 2%, the same effect that would have been brought about by an energy price increase of 11%–20% (Allcott 2011, 1082).

Second, another solution may be the use of generative AI models with the aim of simplifying privacy policies whenever they are displayed, to reduce the cost of reading them. However, this raises the question of how responsibility is to be apportioned in the event that legal action is brought about.

---

10 Article 9 UCPD.

11 Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC, *OJ L* 277/1.

12 Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 PE/17/2022/REV/1 *OJ L* 265/1.

The DSA states that 'providers of online platforms shall not design, organise or operate their online interfaces in a way that deceives or manipulates the recipients of their service or in a way that otherwise materially distorts or impairs the ability of the recipients of their service to make free and informed decisions'.[13] While the phrasing of this article might appear ambitious and extensive, it excludes a significant group of intermediary services from the DSA's restrictions on dark patterns. By limiting the application of Article 25 only to online platforms instead of all intermediary services, the scope of the DSA is narrower than some may expect. As a result, 'a wide range of intermediary services are not subject to the ban', 'including businesses foundational to online commerce, such as ISP's, web-hosting services and domain name registrars' (MacKinnon 2022, 1). This exclusion is arguably a consequential one, given that these intermediary services 'often have consumer-facing businesses'. On the other hand, given that the vast majority of dark patterns are found on large online platforms, it is likely that this scope will be sufficiently broad.

The term 'dark patterns' is never explicitly mentioned or alluded to in the UCPD due to its recency in the field of consumer law. The DSA successfully updates EU law in this aspect. The DSA defines dark patterns on online interfaces of online platforms 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'.[14] It highlights how dark patterns can be used to make the consumer to make decision they do not want to make or to behave in a manner they have not wanted to, which eventually can produce undesirable and negative outcomes for them. As such, the DSA attempts to prohibit all instances of 'deceiving or nudging recipients of the service via the structure, design or functionalities of an online interface or a part thereof'.[15]

A breakthrough by the DSA pertains to its regulations on unfair advertising practices. Misleading advertising constitutes a significant dark pattern which can unduly manipulate and deceive consumers, especially when these advertisements involve targeted information unbeknownst to consumers. Article 26 of the DSA states that online platforms 'shall not present advertisements to recipients of the service based on profiling', and Article 39 highlights additional requirements for online advertising transparency. The UCPD is not easily applicable to advertising practices, even with its vague

13 Article 25(1) DSA.

14 Recital 67 DSA.

15 *Ibid.*

requirement of professional diligence, thus this is undoubtedly a much-needed addition to protect consumers from deceptive advertising. That said, there remain no limitations to diverse forms of micro-targeted online manipulation techniques that enable continuous observation of consumers on the internet for the purposes of online advertising. This is arguably a core issue that is yet to be resolved, which might undermine the rest of the efforts by the Commission in this area.

Overall, the DSA serves to supplement the UCPD in areas where it is lacking, and not to replace it. Thus, regulation of the majority of dark patterns will still fall under the scope of the UCPD's provisions. Further, the DSA is insufficient in furnishing the UCPD's areas of incompletion that were mentioned above. It might be more productive of an endeavour to instead focus on reforming the UCPD's provisions to make them more applicable to dark patterns, as well as for the Commission to issue further guidance incorporating the concept of digital asymmetry.

Moreover, in the European Union, the recently passed Digital Markets Act obliges platforms to refrain from combining data sourced from core platform services with personal data obtained from any other service offered by the gatekeeper or third parties. This is the only solution that seems to take into account the shortfalls of behavioural economics and tries to impair businesses from taking advantage of them. If businesses cannot use the data sourced from core platform services or another service, then the value of settings such as those that hide the collection of location data from consumers will decrease. The solution brought forward by the Digital Markets Act aims at eliminating the market for hidden settings and deceiving choice architecture, rather than intervening to ensure fair competition in this area or facilitating competition in terms of data privacy settings. Although some may argue that this is an over-paternalistic approach, it is submitted that this may be what is needed in the current environment, considering the high cost that consumers are faced with when researching privacy policies. It may be further argued that the large amount of time that would be required to ensure that a consumer is familiar with all the privacy policies makes competition at a data privacy policy level impossible.

8. CONCLUSION

The discussions surrounding online choice architecture and dark patterns are usually focused on the harmful effects of defaults, the difficult nature of procuring consent, or how data is being used for purposes consumers are unaware of. This paper has tried to link the research and show how defaults work towards procuring consent for data processing.

It has been argued that in the current environment, consumers active in online environments where the OCA is dominated by dark patterns should be classified as vulnerable consumers for three reasons. First, the use of defaults vitiates the consumer's ability to consent to privacy policies. Second, consumers are unable to monitor or often even understand how and when data is collected. Third, consumers fail to understand that all the 'free' services are paid with their data. Thus, they fail to compare services and products based on the currency of the online environment: data. It has been explored how, although consumers wish to have more control over their data, they do not invest time into reading privacy policies, which would incentivise businesses to develop better policies. In the absence of a way to incentivise businesses to improve their data policies through competition on the market, several other solutions were explored.

Following this paper, further research into whether showing consumers the profit generated by companies using their personal data would incentivise users to start considering the way that a business handles data as a more important factor in their purchasing decision. In addition, further research into the effects of using generative AI models to simplify consumer policies would be desirable for assessing the suitability of the aforementioned proposal. What is certainly necessary is a reform of the consumer law, to address the consumer law challenges brought about by online choice architecture and dark patterns.

REFERENCES

[1] Allcott, Hunt. 2011. Social norms and energy conservation. *Journal Public Economics* 95: 1082.

[2] BEUC. 2022. "Dark patterns" and the EU consumer law acquis. *BEUC Position Paper*: 1–15.

[3] Competition and Markets Authority (UK). 2022a. Evidence review of online choice architecture and consumer and competition harm. *https://www.gov.uk/government/publications/online-choice-architecture-how-*

digital-design-can-harm-competition-and-consumers/evidence-review-of-online-choice-architecture-and-consumer-and-competition-harm, last visited January 21, 2024.

[4] Competition and Markets Authority (UK). 2022b. *Online Choice Architecture: How digital design can harm competition and consumers.* CMA Discussion Paper.

[5] Duggan, Geoffrey, Stephen Payne. 2011. Skim reading by satisficing: Evidence from eye tracking. *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*: 1141–1150.

[6] Durovic, Mateja, Franciezsck Lech. 2021. A Consumer Law Perspective on the Commercialization of Data. *European Review of Private Law* 29/5: 701–732.

[7] Esposito, Fabrizio, Mateusz Grochowski. 2022. The Consumer Benchmark, Vulnerability, and the Contract Terms Transparency: A Plea for Reconsideration. *European Review of Contract Law* 18/1: 1–31.

[8] European Commission. 2021. Guidance on the interpretation and application of Directive 2005/29/EC of the European Parliament and of the Council concerning unfair business-to-consumer commercial practices in the internal market. *https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021XC1229%2805%29&qid=1640961745514*, last visited December 28, 2023.

[9] Gray, Colin, Yubo Kou, Bryan Battles, Joseph Hoggatt, Austin L. Toombs. 2018. The Dark (Patterns) Side of UX Design. *CHI '18: Proceedings of the Conference on Human Factors in Computing Systems*: 1–14.

[10] Hacker, Philipp. 2021. Manipulation by algorithms. Exploring the triangle of unfair commercial practice, data protection, and privacy law. *European Law Journal* 29/1–2: 142–175.

[11] Jachimowicz, Jon, Shannon Duncan, Elke U. Weber, Eric J. Johnson. 2019. When and why defaults influence decisions: A meta-analysis of default effects. *Behavioural Public Policy* 3/2: 159–186.

[12] Johnson, Eric, Daniel Goldstein. 2023. Do Defaults Save Lives? *Science* 302: 1338–1339.

[13] Kaprou, Eleni. 2023. Aggressive commercial practices 2.0: Is the UCPD fit for the digital age? *EuCML* 12/2: 76–84.

[14] Keller, Punam, Bari Harlam, George Loewenstein, Kevin G. Volpp. 2011. Enhanced active choice: A new method to motivate behaviour change. *Journal of Consumer Psychology* 21/4: 376–383.

[15] Kemp, Katharine. 2023. Your Body, Our Data: Unfair and Unsafe Privacy Practices of Popular Fertility Apps. *UNSW Law Research*: 1–33.

[16] MacKinnon, Eli, King Jennifer. 2022. Do the DSA and DMA Have What It Takes to Take on Dark Patterns? *https://www.techpolicy.press/do-the-dsa-and-dma-have-what-it-takes-to-take-on-dark-patterns/*, last visited January 23, 2024.

[17] Mathur, Arunesh, Gunes Acar, Michael Friedman, Elena Lucherini, Jonathan Mayer, Marshini Chetty, Arvind Narayanan. 2019. Dark patterns at scale: Findings from a crawl of 11K shopping websites. *Proceedings of the ACM on Human-Computer Interaction* 3/CSCW: 1–32. *https://webtransparency.cs.princeton.edu/dark-patterns/*, last visited January 23, 2024.

[18] Sanchez-Rola Iskander, Matteo Dell'Amico, Platon Kotzias, Davide Balzarotti, Leyla Bilge, Pierre-Antoine Vervier, Igor Santos. 2019. Can I Opt Out Yet?: GDPR and the Global Illusion of Cookie Control. *Asia CCS '19: Proceedings of the 2019 ACM Asia Conference on Computer & Communications Security*: 340–351.

Article history:
Received: 20. 12. 2023.
Accepted: 22. 2. 2024.