REPORT OF THE STUDY

ON

"DIGITAL FAIRNESS IN ONLINE RETAIL"

PRESENTED BY

UNIV-PROF DR IUR JÜRGEN KÜHLING, LL.M.

REGENSBURG

AND

CORNELIUS SAUERBORN

RECHTSANWALT (LAWYER)

MUNICH

COMMISSIONED BY

ECOMMERCE EUROPE
EUROCOMMERCE
INDEPENDENT RETAIL EUROPE

REGENSBURG/MUNICH, FINAL REPORT OF 05/09/2024

Structure

A. Background to the commissioning of the study

In 2022, the EU Commission launched a fitness check on EU Consumer Law to examine whether the legal framework can keep pace with current developments in the digital sector in terms of fairness or needs to be revised.[1] It is planning to keep an eye on eventual revisions of the Unfair Commercial Practices Directive (UCPD)[2], the Consumer Rights Directive (CRD)[3] and the Unfair Contract Terms Directive (UCTD)[4]. In addition, consumer associations such as BEUC are calling for existing regulations to be tightened up.[5]

These possible revisions to a balanced system are causing major apprehensions among the representatives from the online retail sector. They are concerned that many of the issues raised are already covered by existing law and that some of the practices that the EU Commission and consumer associations claim to be dangerous play little or no role with online retail and online B2C marketplaces. They are worried that this sector would be unfairly affected by the measures.

This is why they commissioned this study.[6] The purpose of this study is therefore to investigate which of the practices in the reports made available to the EU Commission or the BEUC papers affect online retail and online B2C marketplaces, how frequently they occur, what impact they have and whether they are already covered by EU regulations *de lege lata*. The Report focuses on a restricted and non-exhaustive section of dark patterns, which concerns all digital services such as social networks and not just e-commerce platforms. If regulatory deficits or problems come to light, proposals should be drawn up as to how these can be resolved.

---

1 See https://commission.europa.eu/law/law-topic/consumer-protection-law/review-eu-consumer-law_en.

2 Directive 2005/29/EC.

3 Directive 2011/83/EU.

4 Directive 93/13/EEC.

5 For instance, see *BEUC*, Towards European Digital Fairness, 2023 available at: https://www.beuc.eu/sites/default/files/publications/BEUC-X-2023-020_Consultation_paper_REFIT_consumer_law_digital_fairness.pdf; *BEUC*, "Dark Patterns" and the EU Consumer Law Acquis, available at: https://www.beuc.eu/sites/default/files/publications/beuc-x-2022-013_dark_patters_paper.pdf, *Helberger, Kas, Micklitz, Namyslowska, Naudts, Rott, Sax, Veale*, Digital Fairness for Consumers, 2024, available at: https://pure.eur.nl/ws/portalfiles/portal/139212255/BEUC-X-2024-032_Digital_fairness_for_consumers_Report.pdf, commissioned by BEUC, with numerous considerations, most of which, however, are outside the scope of the UCPD, CRD and UCTD, but concern the new digital laws such as the Data Governance Act, the Digital Services Act, the Digital Markets Act and the AI Act.

6 The authors have already analysed the phenomenon of "dark patterns" in relation to the legal framework in Germany in 2022, see *Kühling/Sauerborn*, Rechtsgutachten über die rechtlichen Rahmenbedingungen sogenannter "dark patterns", available at: https://bevh.org/fileadmin/content/04_politik/Europa/Kuehling-Gutachten-BEVH-Dark-pattern-22-02-16-final.pdf.

B. Facts

The study aims to initially establish the following facts:

1. How can the various practices identified by the report provided with the EU Commission, the CPC network as well as in the reports of BEUC be catalogued and classified?
2. Which of the practices identified are often used in the relevant area of online retail and B2C online marketplaces and to what extent are they used?

In order to clarify these questions, the concept of "digital fairness", which is at the centre of the EU Commission's project, must first be clarified and classified (I.). Then the phenomenon of "dark patterns" and their background, which are the main focus of the debate, must be explained (II.). It is then necessary to define what "dark patterns" represent (III.). The categorisations of "dark patterns" by the individual players is then examined (IV.). Finally, it is necessary to examine which of the practices play a role in online retail (V.).

I. The concept of "Digital fairness" in EU Consumer Law

As the EU Commission's "fitness check" initiative[7] on possible reforms of the UCPD, the CRD and the UCTD is taking place against the background of the term "digital fairness", it is first necessary to clarify what this term means.

Although the concept of digital fairness is very broad and covers, for example, the Digital Markets Act,[8] the General Data Protection Regulation[9] and other new areas such as the AI Act, the term is limited to digital fairness towards consumers due to the areas of regulation to be analysed by the EU Commission. Based on the assumption that there is sufficient fairness in Consumer Law in the offline world, the EU Commission understands digital fairness as equal fairness online and offline.[10] Specific online practices to be analysed with regard to falling under the legal framework according to the EU Commission are consumer vulnerabilities, dark patterns, personalisation prac-

---

7 See https://commission.europa.eu/law/law-topic/consumer-protection-law/review-eu-consumer-law_en.

8 For instance, according to the EU Commission, the aim of the DMA is to "ensure fair and open digital markets", see https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/digital-markets-act-ensuring-fair-and-open-digital-markets_en.

9 See for instance the concept of "fair commercialisation" in Data Protection Law, C. II. 3. a) iii. below.

10 See https://commission.europa.eu/law/law-topic/consumer-protection-law/review-eu-consumer-law_en.

tices, influencer marketing, contract cancellations, subscription service contracts, marketing of virtual items and the addictive use of digital products. These practices need to be examined to determine whether the level of consumer protection that exists offline is equally effective online within the applicable regulatory framework.

Among these numerous practices, especially "dark patterns" were identified as relevant, so that the studies conducted on digital fairness in this context were largely based on studies on these phenomena. This is probably due to the fact that in the online world, consumers communicate with companies via websites and apps whose interfaces – similar to personal persuasion in the offline world – are suitable for influencing consumer[11] choice. This interface design and its potential for consumer manipulation is also precisely the core of "dark patterns".

It should also be noted that "dark patterns" are not a clear-cut phenomenon. The broader the definition of this phenomenon, the more likely it is that other practices that traders use to engage with consumers will also fall under it. For example, the practices of "contract cancellations" mentioned by the EU Commission, the aggravation of which as a *roach motel* pattern also takes place in the course of the investigations of "dark patterns". Personalisation practices, which by their very nature are related to Data Protection Law, are also discussed under the aspect of "dark patterns".[12] Furthermore, influencer marketing with concealment of the advertising character of paid contributions can fall under the *disguised ads* pattern. Finally, "dark patterns" exploit consumer vulnerabilities such as attention deficits,[13] meaning that the concept of consumer vulnerabilities is also closely intertwined with the discourse on "dark patterns".

For this reason, in accordance with a broad definition of the term "dark patterns", this study will focus on the categorisation and legal assessment of these phenomena.

II. "Dark patterns" and their background

Techniques to promote sales have been used for some time in the interaction between traders and consumers. From the consumer's point of view, this has not always been *fair*. Deceitful sales techniques, such as *bait-and-switch* offers, were documented in China as early as the beginning of the

---

11 When analysing the phenomenon, the focus is typically placed on the consumer as a legal concept. Such an understanding is not mandatory, as entrepreneurs can also be addressees of "dark patterns". For more on this, see III.1.

12 See *Kühling/Sauerborn*, Rechtsgutachten über die rechtlichen Rahmenbedingungen sogenannter "dark patterns", p. 48 et seq., available at: https://bevh.org/fileadmin/content/04_politik/Europa/Kuehling-Gutachten-BEVH-Dark-pattern-22-02-16-final.pdf.

13 See III. below.

17th century.[14] However, the actual practice is probably much older. Just think of market criers who advertised the properties of their goods, some of which they did not even possess.[15]

Even in the modern world, the design of websites is intended to promote sales. The Internet in particular offers a wide range of opportunities to influence customers and encourage them to purchase additional goods or services. Modern means of data processing allow that offers can be tailored to the individual user in a more personalised way than ever before – and this also increases the risk of subliminally influencing consumers. In recent times, the term "dark patterns" has been used in this respect to flag allegedly harmful practices. The term was coined in 2010 by the US American Harry Brignull.[16] However, it is a collective term without fixed contours. Incidentally, influencing consumers is also commonplace in the "analogue" world. For example, nothing is left to chance in the presentation of goods in supermarkets. In the fruit and vegetable department, for instance, warmer colours can be found and increased air humidity through diffusers is intended to make the goods appear fresher. Higher-priced items are often displayed at eye level, while lower-priced alternatives are placed further down.

Nevertheless, the term "dark patterns" has become a kind of battle cry for consumer protection in the digital environment. As a result of the increasing popularity of the term, the EU Commission felt compelled to launch investigations into "digital fairness". To this end, it commissioned a study to examine "dark patterns and manipulative personalisation" in the digital environment.[17] This detailed study identified numerous practices as "dark patterns" and found numerous examples of them across all sectors.

In addition, the EU Commission used the CPC Network[18] to search for practices commonly known as "dark patterns" in the EU member states. The CPC Network checked 399 online shops for untrue

---

14 Examples in *Zhang Yingyu*, The Book of Swindles, 2017.

15 See also *Helberger, Kas, Micklitz, Namyslowska, Naudts, Rott, Sax, Veale*, Digital Fairness for Consumers, 2024, available at: https://pure.eur.nl/ws/portalfiles/portal/139212255/BEUC-X-2024-032_Digital_fairness_for_consumers_Report.pdf, p. 194, pointing this out.

16 *Brignull*, Dark Patterns: dirty tricks designers use to make people do stuff, 8/7/2010, available online: https://90percentofeverything.com/2010/07/08/dark-patterns-dirty-tricks-designers-use-to-make-people-do-stuff/.

17 *Lupiáñez-Villanueva/Boluda/Bogliacino/Liva/Lechardoy/Rodríguez de las Heras Ballell*, Behavioural study on unfair commercial practices in the digital environment, 2022, available at: https://op.europa.eu/en/publication-detail/-/publication/606365bc-d58b-11ec-a95f-01aa75ed71a1/language-en/format-PDF/source-257599418.

18 "Consumer Protection Cooperation Network", a network of national consumer authorities according to Regulation 2017/2394.

countdown timers, *hidden information* and *misdirecting* consumers. Approximately 40% of the websites checked exhibited such practices.

The relevance of such "dark patterns" raises numerous legal questions. In particular, the consumer organisation BEUC is campaigning for a comprehensive reform of Consumer Law provisions, as it states that the current legal framework is not sufficient to effectively counter "dark patterns".[19]

Some trade associations representing companies active in online retail are rather cautious about the planned reform proposals and are concerned that the compliance requirements for companies are too high. After all, many of the practices that have been identified have no relevance in online retail and are more relevant in other sectors. They fear that there would be too much regulatory overreach, which could lead to compliance requirements in the retail sector becoming almost unmanageable hurdles and few benefits to consumers. They also question whether a reform of the legal framework is necessary at all, as there is already a high level of consumer protection in the EU which is already covering "dark patterns". There is rather a lack of effective instruments for enforcing consumer rights than a lack of provisions.[20]

III. Definition of "dark patterns"[21]

Before discussing how the current legal framework deals with "dark patterns", the phenomenon must be defined beyond the legal context.[22]

Due to the increasing use of the term "dark patterns" in studies and legislative projects, many attempts have been made to define it. However, it is by no means easy to narrow down the problem precisely. This is due to the fact that the manipulative design of interactions with people is a constantly changing practice that can be completely different depending on the environment and is constantly being adapted, especially in the digital sector. It is also difficult to differentiate between "dark patterns" and general influence being common in interpersonal communication. However, a

---

19 For instance, *BEUC*, "Dark Patterns" and the EU Consumer Law Acquis, p. 5 et seq., available at: https://www.beuc.eu/sites/default/files/publications/beuc-x-2022-013_dark_patters_paper.pdf.

20 For instance *Ecommerce Europe,* Ecommerce Europe's reply to the Call for evidence on Digital Fairness – fitness check on EU Consumer Law, available at: https://ecommerce-europe.eu/wp-content/uploads/2022/06/ECOM-Final-reply-call-for-evidence-digital-fairness-14062022.pdf.

21 This section is based on the findings of *Kühling/Sauerborn*, Rechtsgutachten über die rechtlichen Rahmenbedingungen sogenannter "dark patterns", p. 14 et seq., available at: https://bevh.org/fileadmin/content/04_politik/Europa/Kuehling-Gutachten-BEVH-Dark-pattern-22-02-16-final.pdf.

22 A discussion of whether the legal framework sufficiently addresses "dark patterns" can be found in C. below.

clear definition is of considerable relevance, as the term "dark patterns" has strong negative connotations and practices labelled as "dark patterns" are already subject to a prohibition debate *per se*, as they are connoted as being *unfair* and might be causing harm, while influences that are considered *fair* must be permitted. In addition, there are some calls for a complete ban on "dark patterns",[23] which further increases the need for legitimisation of a concrete definition.

There is general agreement that "dark patterns" are interactions with people that are intended to push or tempt the person to make an undesirable decision, harming the consumer.[24] "Dark patterns" are thus characterised by three core elements. The "dark pattern" must interact with a person, this person must be induced in some way to take an action, and this action must run counter to the person's (supposed) interests. In the following, these requirements must be specified in order to develop a suitable definition of "dark patterns".

1. Addressee of "dark patterns"

It is typically assumed that the person addressed by "dark patterns" is a consumer. At first glance, this understanding is not compelling. However, "dark patterns" follow the idea of influencing the addressee, which is likely to be particularly noticeable in the case of consumers. According to case law, traders must apply a heightened level of attention in commercial transactions, which is why they are expected not to allow themselves to be misled into irrational behaviour.[25] This is also supported by the fact that Consumer Law only requires a reasonably attentive consumer,[26] so that attention deficits are being addressed by Consumer Law. Therefore, from a normative point of view, traders must categorically not be susceptible to "dark patterns". In addition, the examples usually cited, all of which are tailored to consumers, also suggest that "dark patterns" are a phenomenon that occurs exclusively in the interaction with consumers. It can therefore be assumed that in the context of this study, the addressees of "dark patterns" are consumers only.

---

23 For example *BEUC*, Towards European Digital Fairness, 2023 available at: https://www.beuc.eu/sites/default/files/publications/BEUC-X-2023-020_Consultation_paper_REFIT_consumer_law_digital_fairness.pdf. They carefully suggest "a horizontal ban on dark patterns", see p. 13.

24 See, for example, Recital 50a of the Digital Services Act, Regulation 2022/2065 in its compromise draft. The wording is not included in the final version of the DSA. See also *Martini/Drews/Seeliger/Weinzierl*, Zeitschrift für Digitalisierung und Recht (ZfDR) 2021, 47, 49, footnote 10 with further references.

25 See for instance *German Federal Court of Justice (BGH)*, judgement of. 19/4/2018 - I ZR 154/16, para. 71 – *Werbeblocker II.*

26 More on the consumer model see C. I. 1. a) below.

2. Influencing effect

"Dark patterns" also have an influencing effect. This is a characteristic, yet very broad term for "dark patterns", as almost any interaction with another person will potentially influence their actions. It is sometimes assumed that the degree of influence is decisive for the categorisation of a practice as worthy of prohibition. For example, (prohibited) manipulation under Art. 25 DSA[27] is deemed to exist if the user would not have made the specific decision without the influencing design of the website.[28] The effectiveness of some practices is also discussed in the study assigned by the EU Commission against the background of influence,[29] whereby greater effectiveness is measured by the fact that users made a different decision when using an influencing practice than without this influence.

However, to accept the mere influence as a characteristic is a circular argument. The interaction of economic entities, in particular the advertising of goods and services, is essentially based on the idea of influencing the addressees. In the analogue world, for example, a car salesman who sells the customer the car he or she would have bought anyway would do an unnecessary job. An advert that only shows goods or services that the addressee would have bought anyway would be ineffective and worthless. Mere influenceing, which is ubiquitous, is therefore not sufficient to define "dark patterns". This is also in line with the UCPD, which covers unfair commercial practices which directly harm consumer' economic interests and thereby indirectly harm the economic interests of legitimate competitors[30] in addition to the mere influence of an act on the consumer's.[31]

Attempts have therefore been made to specify the influence that characterises "dark patterns". *Harry Brignull*,[32] , who coined the term "dark patterns", considers the prerequisite to be that the influence occurs through the utilisation of specific knowledge about human decision-making processes. *Arunesh Mathur*[33] is of the opinion that "dark patterns" are characterised by changing the

---

27 Digital Services Act, Regulation 2022/2065.

28 *Martini/Kramme/Kamke*, (Multimedia und Recht) MMR 2023, 323, 324.

29 *Lupiáñez-Villanueva/Boluda/Bogliacino/Liva/Lechardoy/Rodríguez de las Heras Ballell*, Behavioural study on unfair commercial practices in the digital environment, 2022, p. 85 et seq., available at: https://op.europa.eu/en/publication-detail/-/publication/606365bc-d58b-11ec-a95f-01aa75ed71a1/language-en/format-PDF/source-257599418.

30 See Recital 6 and Art. 1 UCPD

31 See C. II. 2. below.

32 *Harry Brignull* is conducting research on the design of user interfaces and manages the website "darkpatterns.org".

33 *Arunesh Mathur* is a Postdoctoral Research Fellow at the Center for Information Technology Policy at Princeton University.

decision architecture of the addressee, either by manipulating the flow of information (such as by omitting expected information) or by influencing the decision space (such as with differently designed buttons).[34] It must therefore not be the "if" of the influencing mode of action, but the "how" that is decisive. The core issue must therefore be whether the communication with the consumer is deliberately developed in such a way that human behaviour patterns such as inattention, convenience or the existence of prior expectations are unfairly influenced, and the decision flow is thus steered by the specific design.

This in turn raises difficulties in differentiating it from so-called *convenient design*. Cases are conceivable in which the design of the user interaction has an influencing effect, but this leads to the user perceiving the design as particularly user-friendly. For example, the simple selection of particularly frequently chosen options on the first level of an interface, with further options on a second level, can also lead to an enhanced user experience.

The most sensible approach to this problem is to prioritise user autonomy. Influencing would reach an unfair level if the consumer makes a decision based on the influence that he or she does not actually support internally. In this case, the control question to the consumer would be: "Did you really want that?". This excludes cases in which the trader has influenced a decision but nevertheless, the consumer made it of their own volition.[35] Against this background, when analysing the influencing effect, it can be considered whether the consumer can reverse the decision by the simplest means.

3. Ignorance of consumer interests

The third core element of "dark patterns" is that the action is only advantageous for the trader. This element, which is intended to characterise "dark patterns", is often understood to mean that the action must be disadvantageous for the consumer. However, this is not a criterion that can be used to draw a distinction, as it is strictly subjective and is therefore hardly suitable as a generalisable, objective determination criterion. What is undesirable for one person may very well be desirable

---

[34] *Weinzierl*, MMR-Aktuell 2021, 440222, who reports on the FTC workshop on "dark patterns", at which *Harry Brignull* and *Arunesh Mathur* were speakers.

[35] See *Glöckner*, in: Harte-Bavendamm/Henning-Bodewig (eds.), Commentary of the German Unfair Commercial Practices Act (UWG), 5th ed. 2021, Instruction, paras. 487 et seq.; see *Kühling/Sauerborn*, Rechtsgutachten über die rechtlichen Rahmenbedingungen sogenannter "dark patterns", p. 42 et seq, available at: https://bevh.org/fileadmin/content/04_politik/Europa/Kuehling-Gutachten-BEVH-Dark-pattern-22-02-16-final.pdf.

for another. But even the preferences of one and the same person can change.[36] Focusing on the meaningfulness of an action in the sense that the benefits for the consumer are to be determined is also not expedient, as irrational decisions can also be entirely desirable for the individual.[37] One solution is to focus primarily on the trader. "Dark patterns" do not necessarily acquire their *dark* aspect because they run counter to the interests of the consumer, but above all because the trader uses them unilaterally for their own purposes. The correct approach is therefore to focus on the provider of "dark patterns" when assessing the action being taken. "Dark patterns" are therefore characterised by the fact that they are used unilaterally by the trader without taking into account supposed user interests so that the trader benefits from the influenced actions.[38] Against this background, measures cannot constitute "dark patterns" to which the trader is legally obliged. The trader is not pursuing a unilateral interest for such measures, but the interest of the legislator.

4. Distinction from nudging

This also raises the question of how to distinguish it from "nudging", which has predominantly positive connotations. These are also influencing techniques, but they are intended to meet the anticipated preferences of the addressee or pursue public interests,[39] as they are, among other things desired on the legislative side by the Empowering Consumers for the Green Transition Directive.[40] Convenient design could also be categorised as such.[41] The special emphasising of sustainable products, called "green nudging" is also discussed.[42] The aim of pursuing desirable interests through "nudging" in particular raises complicated questions of demarcation from "dark patterns", as the provider of control mechanisms can also pursue their own interests in addition to desirable aims.[43] If such steering measures are therefore excluded from the area of "dark patterns" from the

---

36 *Martini/Drews/Seeliger/Weinzierl*, ZfDR 2021, 47, 52, refer to this.

37 Think of the many self-harming behaviours, such as tobacco or alcohol consumption, of which consumers are well aware of the possible consequences.

38 This is the characteristic abusive aspect of "dark patterns", see *Martini/Drews/Seeliger/Weinzierl*, ZfDR 2021, 47, 52, 53. This idea is also correctly expressed in Art. 5 (2) UCPD, see C. II.2. e) below.

39 See *Loy/Baumgartner*, Zeitschrift für Datenschutz (ZD) 2021, 404 with further references.

40 See the provisions on special labelling of environmentally friendly behavioural alternatives in the Proposal of the European Parliament and the Council on such a Directive, available at: https://data.consilium.europa.eu/doc/document/ST-5417-2024-INIT/en/pdf. For further information, see *Jung/Dowse*, Verbraucher und Recht (VuR), 2023, 283.

41 See 2. above.

42 See *Frauenhofer ISI*, Studie zur Oekologischen Nachhaltigkeit des Onlinehandels in Deutschland (OeNO-Studie), p. 99, available at: https://bevh.org/fileadmin/content/04_politik/Nachhaltigkeit/OENO/OENO_Fraunhofer_ISI_Oekologische_Nachhaltigkeit_Onlinehandel_Final_BEVH-WEB.pdf.

43 For example, it is possible to prevent a high returns rate with an online retailer by making the return conditions more difficult, which on the one hand should be in the public interest of environmental protection, but on the other hand also brings (considerable) savings for the trader.

outset, there is a risk that public welfare interests will be put forward so that measures that are nevertheless unilaterally favourable to the trader can be implemented. In addition, it is not the task of companies interacting with consumers to enforce public welfare interests through manipulative design regardless of the will of the consumer. In order not to exclude designs whose manipulative effect may also serve public welfare interests by chance or pretence from a critical examination from the outset, such designs must also be conceptually qualified as "dark patterns". On the other hand, an examination of interests that do not only serve the trader must be carried out within the individual regulatory elements. It should also be noted that the development of a taxonomy of legitimate public interests is already confronted with considerable difficulties even at national level, and this applies even more so at Union level.

This means that "dark patterns" are also to be regarded as such interaction designs that actually or supposedly have a charitable effect or satisfy the interests of the addressee, as long as they are at least also used to unilaterally serve the interests of the trader. Whether such practices are to be prohibited is then a question of the threat to the consumer autonomy or the existence of a justification in the individual case. Conversely, however, such patterns are unobjectionable if they are only intended to serve the interests of users or the common good without favouring the trader. Since, as already mentioned, such a demarcation is difficult, legal certainty must be ensured here. Therefore, it seems more sensible to explicitly authorise nudging by means of soft law or legislation if it is to be desired in individual cases and to otherweise be subject to the general legal framework on "dark patterns".

5. Restriction to the online world?

Many examples of "dark patterns" can be found when interacting with services presented on websites. However, the definition of "dark patterns" is not necessarily limited to the online world. Numerous examples of one-sided influencing interactions can also be found in the offline world, such as in the design in stores or artificial odours,[44] but also in brochure advertising alone. Historical practices of influence dating back to a time before the Internet can also be defined as "dark patterns".[45] Such are therefore not a purely online phenomenon and should not be limited to this definition.

[44] See also *Martini/Drews/Seeliger/Weinzierl*, ZfDR 2021, 47, 50 with further references.
[45] See II. above.

6. Interim results

As a result, "dark patterns" can be defined as follows: They are all forms of interaction, whether online or offline, which are aimed at consumers and objectively take advantage of human behaviour with the purpose of enforcing the trader's unilateral interests without considering the interests of the addressee, regardless of whether they are also pursuing any public interests.

However, it should be emphasised that a definition of "dark patterns" does not yet make any statement as to whether such behaviour is or should be within the scope of permitted communication or prohibited influence. Even after a definition, the concept of "dark patterns" is not sufficiently clear and can hardly be sufficiently differentiated from general, permitted influence to be used as a benchmark for the prohibition of a behaviour. According to the definition above, the term "dark patterns" would also include so-called "quenching goods": The arrangement of goods in stores is an interaction design that is aimed at consumers and takes advantage of the shortened patience of shoppers. Nevertheless, there is no discussion about the prohibition of such a practice against the background of UCPD reform programs. Classifying a phenomenon as a "dark pattern" therefore does not exempt the creation of legal provisions from examining whether or not the respective behaviour should be prohibited against the background of the fundamental rights and freedoms of companies as well as data and consumer protection.

IV. The practices identified as "dark patterns" impeding digital fairness

1. The study assigned by the EU Commission

In April 2022, the EU Commission published a study it assigned with the title "Behavioural study on unfair commercial practices in the digital environment: dark patterns and manipulative personalisation".[46] The study aims to systematically and completely identify problematic practices in the B2C sector, highlight the effects of these practices on consumers and make recommendations for reform proposals. The experts carried out specific test purchases and were thus able to compile a collection of numerous practices with concrete evidence.

[46] *Lupiáñez-Villanueva/Boluda/Bogliacino/Liva/Lechardoy/Rodríguez de las Heras Ballell*, Behavioural study on unfair commercial practices in the digital environment, 2022, available at: https://op.europa.eu/en/publication-detail/-/publication/606365bc-d58b-11ec-a95f-01aa75ed71a1/language-en/format-PDF/source-257599418.

When categorising the practices, the experts drew on practices already known to various researchers. Firstly, the studies by *Harry Brignull,* who coined the term "dark patterns", is to be mentioned.[47] Other sources are in particular the studies by *Bösch/Erb/Kargl/Kopp/Pfattheicher*[48]*, Gray/Kou/Battles/Hoggatt/Toombs*[49] and *Mathur/Acar/Friedman/Lucherini/Mayer/Chetty/Narayanan*[50]. In addition, several papers from authorities were analysed that contain further groups of cases. These were categorised according to various criteria, for example into the groups "Information Asymmetry" and "Free Choice Repression" or grouped practices that fall under the categories "Choice Architecture" and "Decision-Making".

The most relevant categories of "dark patterns" from the study are:

- *Nagging* (Repeated and persistent requests to do something the online company prefers)
- *Social proof*:
    - *Activity messages* (Misleading notice about other consumers' actions, such as "10 people are currently viewing this offer")
    - *Testimonials* (Misleading statements from fake or real consumers, in particular fake customer reviews)
- *Obstruction*:
    - *Roach motel*/*difficult cancellations* (Asymmetry between signing up (easy) and cancelling (hard))
    - *Price comparison prevention* (Frustrates comparison shopping, such as confusing price indications per quantity or similar)
    - *Intermediate currency* (Purchases in virtual currencies to obscure costs)
- *Sneaking*:
    - *Sneak into basked* (Items that consumers did not add end up in the cart)
    - *Hidden costs* (Costs obscured or disclosed late in the transaction)
    - *Hidden subscription*/*Forced continuity* (Unanticipated or undesired automatic renewal)
    - *Bait and switch* (Consumers are sold something different from what originally advertised/A different action is performed than the interface suggests)

---

47 Available at: https://www.darkpatterns.org/types-of-dark-pattern.

48 *Bösch/Erb/Kargl/Kopp/Pfattheicher*, Tales from the Dark Side: Privacy Dark Strategies and Privacy Dark Patterns, available at: https://petsymposium.org/2016/files/papers/Tales_from_the_Dark_Side__Privacy_Dark_Strategies_and_Privacy_Dark_Patterns.pdf.

49 *Gray/Kou/Battles/Hoggatt/Toombs*, The Dark (Patterns) Side of UX Design, available at: https://dl.acm.org/doi/pdf/10.1145/3173574.3174108.

50 *Mathur/Acar/Friedman/Lucherini/Mayer/Chetty/Narayanan*, Dark Patterns at Scale: Findings from a Crawl of 11K Shopping websites, available at: https://arxiv.org/pdf/1907.07032.pdf.

  - *Address book leeching* (Coercing the user to share their contacts' personal data in order to use the service)
- *Interface interference*:
  - *Hidden information/False hierarchy* (Important information visually obscured or ordered in a way to promote a specific option; This is to be distinguished from nudging in the sense of convenient design.[51] Suggestions that are displayed to the customer because they correspond to their supposed interests are not "dark patterns" *per se*)
  - *Hidden costs* (Costs obscured or disclosed late in the transaction)
  - *Preselection (default)* (Preselected option that is in the trader's interest)
  - *Toying with emotions* (Emotionally manipulative framing of the design)
  - *Trick questions* (Intentional or obvious ambiguity to confuse consumer, such as double negations)
  - *Disguised ads* (Consumer induced to click on something that is not clearly an advertisement, such as alleged press reports that are actually advertising)
  - *Confirmshaming* (Choice framed in a way that seems dishonest/foolish for consumer)
- *Forced action*:
  - *Forced registration* (Consumer tricked into thinking registration is necessary)
- Urgency:
  - *Low stock/High demand message/Scarcity* (Consumers falsely informed of limited quantities)
  - *Countdown timer/Limited time message* (Opportunity ends with false visual information on offer period)

Based on these case groups, the researchers analysed websites from France, Ireland, Germany, Austria, the Netherlands, Belgium, Italy, Norway and Portugal and presented the results in tabular form.

2. "Dark patterns" in the sweep of the CPC network

The case groups on which the sweep of the CPC network from 2022[52] was based are far less diversified. This was limited to the following case groups:

- *Fake countdown timers*

[51] See III. 4. above.

[52] See press release of 30/01/2023, available at: https://ec.europa.eu/commission/presscorner/api/files/document/print/en/ip_23_418/IP_23_418_EN.pdf.

- *False hierarchy*
- *Hidden information*

These categories of "dark patterns" are already included in the taxonomy of the study assigned by the EU Commission[53] and therefore do not need to be reexplained. However, it is worth noting that the study related to online shops and corresponding apps, meaning that the results are particularly relevant for the sector analysed with this study.

3. "Dark patterns" according to BEUC

BEUC also analyses categories of "dark patterns".[54] They consider that individual categories of "dark patterns" are differentiated according to whether they (1) emphasise individual decision-making options or make them easier, (2) create a false sense of urgency or scarcity and thus promote a "fear of missing out", (3) originate from consumers, for example by subjecting them to a sense of social influence or peer pressure, (4) obstruct or confuse consumers and finally (5) blind consumers.

BEUC thus draws on the well-known taxonomy of "dark patterns", for example by *Mathur et al.*, which was also the basis of the investigation in the study assigned by the EU Commission.[55] It can therefore be referred to above for the individual categories.

4. Interim result

The studies reflect the already known taxonomy of "dark patterns". Overall, it is noticeable that these examples are likely to be predominantly relevant in the online world, but some also have counterparts in the offline world. For example, "dark patterns" based on emotional influence, such as *confirmshaming*, are likely to occur in the same way in the offline world, as direct human contact is generally much more susceptible to emotional influence than quasi-anonymous contact in the online world. The same applies to other "dark patterns", such as *forced registration* that also exists at newspaper stands with subscription traps in exchange for a small gift for the subscriber, *scarcity* that always resonates as a thought during sales or *nagging* during particularly intensive customer contact by hoover representatives.

---

53 See 1. above.

54 *BEUC*, "Dark Patterns" and the EU Consumer Law Acquis, p. 5 et seq., available at: https://www.beuc.eu/sites/default/files/publications/beuc-x-2022-013_dark_patters_paper.pdf.

55 See 1. above.

It must be noted that "dark patterns" is a moving target. The practices found should therefore only ever be seen as a momentary picture and can be expanded to include new practices at any time. It is also conceivable that individual practices may lose relevance because they have been banned and their ban has been effectively enforced, or because they have been replaced by more effective new practices. A categorisation of "dark patterns" can therefore only be an aid to identifying relevant practices and investigating whether they are worthy of prohibition. However, categorisation can in no way replace a legal examination.

This confirms that "dark patterns" do not trigger a need for prohibition *per se* but can in some cases be permitted influence. It can therefore be said that "dark patterns" contain a *dark* core that can be characterised as unfair and trigger a need for a ban. However, there is an area around this core that does not trigger this need inherently, but must be accessible to a certain degree of consideration. Once again, *confirmshaming* is to be mentioned as an example, where the boundary between an acceptable emotional appeal and an unacceptable emotional influence is fluid and depends on a variety of factors, such as the cultural background of consumer habits, which is likely to differ in the EU Member States. This will be further discussed in the legal assessment.[56]

V. Relevance of the examples found for the online retail sector

Now that "dark patterns" have been defined and the practices listed in the relevant reports are documented, it is necessary to analyse whether these practices are relevant to the online retail sector. BEUC does not mention any practices that are specifically relevant to online retail.[57]

1. Relevant practices according to the CPC network's sweep

As already discussed,[58] the results of the CPC network's sweeps on "dark patterns" are concerning the online retail sector, as the research was based only on this particular sector. However, the specific cases of the CPC network are not disclosed so that they cannot be verified. Only the number of cases is published:[59]

- Fake countdown timers: 42 of 399 web shops
- False hierarchy: 54 of 399 web shops

---

56 See C. below.

57 For a detailed analysis of the legal framework adressing these examples, see C. below.

58 See IV. 2. above.

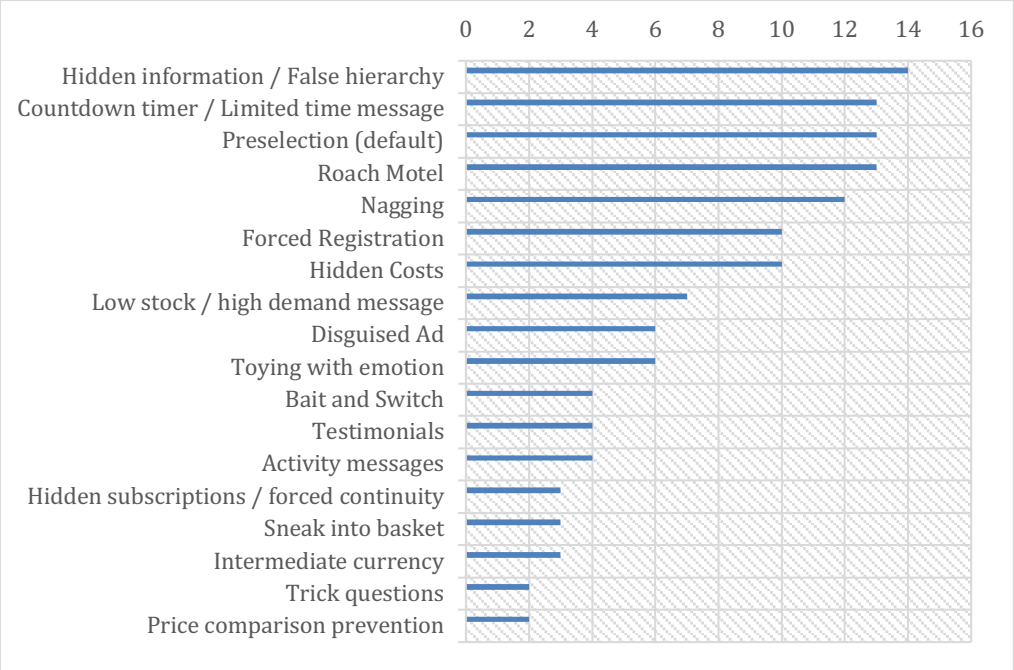
59 It should be noted that the CPC network's sweep does not contain any information on individual shops. It is therefore not possible to draw any conclusions regarding the relevance of the results found, particularly with regard to the potential number of consumers who have visited these websites or apps.

- Hidden information: 70 of 399 web shops
- "Dark patterns" in shopping apps: 27 of 102 apps

2. Relevant practices according to the study assigned by the EU Commission

However, the study assigned by the EU Commission is different.[60] It cites specific investigations, so that these can be scrutinised more closely. Nevertheless, it should be noted that the study was conducted across all sectors, meaning that it is first necessary to filter which cases are relevant for online retail and B2C marketplaces.

But the study itself already takes this into account. From page 46 onwards, the study carries out sector-specific analyses of "dark patterns", focusing specifically on online marketplaces and e-commerce. The study was based on 29 websites from this particular sector. Figure 3[61] shows the total number of the various forms of "dark patterns" found on marketplaces and ecommerce web-sites and apps:[62]



60 See IV. 1. above.

61 *Lupiáñez-Villanueva/Boluda/Bogliacino/Liva/Lechardoy/Rodríguez de las Heras Ballell*, Behavioural study on unfair commercial practices in the digital environment, 2022, p. 46, available at: https://op.europa.eu/en/publication-detail/-/publication/606365bc-d58b-11ec-a95f-01aa75ed71a1/language-en/format-PDF/source-257599418.

62 *Lupiáñez-Villanueva/Boluda/Bogliacino/Liva/Lechardoy/Rodríguez de las Heras Ballell*, Behavioural study on unfair commercial practices in the digital environment, 2022, p. 46 et seq., available at: https://op.europa.eu/en/publication-detail/-/publication/606365bc-d58b-11ec-a95f-01aa75ed71a1/language-en/format-PDF/source-257599418.

The following categories and examples of "dark patterns" are documented in the study:

a) Countdown timer/Limited time message

Firstly, the study lists examples in which the researchers found *countdown timers* or *limited time messages*. However, these are not elaborated on further, except for one example.[63]

The study only contains statements to the effect that the countdown was "false", i.e. that the offer remained almost unchanged after the countdown expired. As the study rightly notes (and this is also in line with the situation under the UCPD)[64], a *countdown timer* is only a "dark pattern" if the countdown is false, which means, that its end does not lead to a consequence. The existence of a countdown, as covered by a screenshot, therefore does not automatically mean that a "dark pattern" is shown. This is because it is conceivable that an offer may actually end after the countdown has expired, meaning that the countdown is true. The mere (true) expiry of an offer is not sufficient to constitute a "dark pattern". For example, with auctions, a *countdown* is no "dark pattern" even if the bidding page is visited very late, shortly before the auction closes, as indeed no more bids are accepted after the *countdown* has ended. The study does not investigate whether the *countdown* also expired without consequences on websites other than the one mentioned, so it is conceivable that the other examples are not "dark patterns".

b) Activity Messages

The study then takes a look at *activity messages*, i.e. showing the (supposed) behaviour of other customers. As the study itself points out, the truthfulness of these messages is also an important criterion when categorising *activity messages* as "dark patterns". Therefore, according to the study itself, it is conceivable that there were no "dark patterns" in the examples found.

c) Forced Registration

The study found *forced registration* patterns on some websites and in some apps that could not be used if personal data such as a telephone number or an email address was provided.

---

63 *Lupiáñez-Villanueva/Boluda/Bogliacino/Liva/Lechardoy/Rodríguez de las Heras Ballell*, Behavioural study on unfair commercial practices in the digital environment, 2022, Figure 4, p. 47, available at: https://op.europa.eu/en/publication-detail/-/publication/606365bc-d58b-11ec-a95f-01aa75ed71a1/language-en/format-PDF/source-257599418.

64 See C. II. 2. a) below.

d) Hidden subscription/Forced continuity

The study claims to have found some *hidden subscription* or *forced continuity* patterns. As an example, it shows a credit card, where the customer receives a discount of EUR 40 of their current order when applying for the card, which is why the purchase might in the end even be free. However, the terms and conditions of the credit card state that only the first year is free, but that a fee of EUR 20 is charged for each subsequent year.

It is surprising that this specific credit card is mentioned as an example of a *hidden subscription* pattern, as the conclusion of a credit card contract is initially a very complex endeavour involving identity checks and the conclusion of a contract with a variety of mandatory information. It is therefore questionable to what extent the conclusion of a credit card contract is supposed to be *hidden*. Therefore, it is doubtful whether the study actually revealed *hidden subscription* patterns or whether the experts applied a standard too broad when assessing "dark patterns".

e) Roach motel

During the test purchases, the study claims that several websites were identified where it was difficult to delete the user account. In some cases, support had to be contacted. On some online retail sites, registering premium models was also much easier than deleting the account, which even required a tutorial for deletion. This identified *roach motel* patterns.

f) Nagging

The study states that it has identified a larger number of *nagging* patterns, for example to buy specially recommended products or persistent promotions for special offers and discounts as well as to activate notifications.

g) Hidden costs

The study also states that it has identified *hidden cost* patterns. For example, numerous online shops would only indicate the total costs in the final ordering step. One retailer is highlighted in particular, where the option "collect at store" is said to cost EUR 9.90, even though the product was on site and only cost EUR 3.40.

It is doubtful whether this practice constitutes a "dark pattern". After all, the price is stated transparently at the end of the ordering process. The particular amount of the fee when opting to collecting goods from the store is also unlikely to constitute a *hidden cost* pattern. What the shop charges is irrelevant when assessing whether a behaviour is an unfair pattern, as long as this is done in a sufficiently transparent and complete manner. Once again, this shows a possibly overly broad understanding of what can be identified as a "dark pattern". It is therefore questionable which of the practices identified in the study actually qualify as such.

h) Disguised ads

The study also identified some disguised ads. One example shows a list of products, with an advert for a motor vehicle labelled "Ann." is shown. Whether the specific design due to the labelling "Ann." for "Annunci", which means "advertisement", actually constitutes a *disguised ads* pattern depends on whether the concrete design is sufficiently recognisable as an ad. There is good reason to assume that this is the case, as in addition to the labelling, the format of the ad also differs from the other page content (the ad is narrower compared to the other items, there is no heart on the right-hand side to flag the item as a favourite, there is no display of a price). Nevertheless, this is a borderline case, so it is also conceivable to assume a *disguised ads* pattern here.[65]

i) Toying with emotions

The study then mentions *toying with emotions* patterns that the researchers have identified on some websites or apps. For example, an extended warranty was allegedly advertised by warning the user that a repair without a warranty could cost over EUR 100. Another example, among others, is, showing the message "We are very sad to say goodbye to you" when deactivating an account. The latter is an example of a possible *confirmshaming* pattern that requires special consideration in legal terms.[66]

j) Bait and switch

According to the study, *bait and switch* patterns were also found. A website recommended other products than those that were being searched for. Whether these practices actually constitute *bait and switch* patterns cannot be verified due to the lack of provided examples. In any case, simply

[65] See C. II. 2. a) below.
[66] See C. II. 2. b) and C. III. 2. b) vi. below.

recommending products other than those searched for does hardly constitute a *bait and switch*, as it contains its *dark* moment in that an interaction leads to the execution of a different action than expected.[67] The mere display of alternative suggestions is unlikely to fulfil this requirement. In addition, these could rather be *false hierarchy* patterns, whereby it would have to be considered whether the hierarchy corresponds to the supposed wishes of the customers, which would argue against the existence of a "dark pattern".[68]

k) Sneak into basket

The study also found *Sneak into basket* patterns. For example, when ordering a piece of furniture, an insurance policy is said to have been automatically placed in the shopping basket, which would have had to be removed by the user.[69] Such a *sneak into basket* pattern also represents a *preselection* pattern.

3. Interim result

It has proven to be evident that "dark patterns" have a certain relevance in the sector of online retail and B2C marketplaces. However, not all categories of practices are actually relevant in this sector. "Dark patterns" concerning data protection aspects such as *address book leeching* were not found in the particular sector.

In addition, the total number of practices that are relevant for online retail is difficult to determine. The studies submitted to the EU Commission either do not show any verifiable examples, or if they do, they show a very broad interpretation of the term "dark patterns" and in some cases assume their existence without being able to examine the relevant conditions of the exact category in more detail. This concerns, for example, the question of whether a countdown is *false*, which is relevant for the categorisation of a countdown as a "dark pattern".[70]

---

67 See *Kühling/Sauerborn*, Rechtsgutachten über die rechtlichen Rahmenbedingungen sogenannter "dark patterns", p. 19, available at: https://bevh.org/fileadmin/content/04_politik/Europa/Kuehling-Gutachten-BEVH-Dark-pattern-22-02-16-final.pdf.

68 See IV. 1. above.

69 On such a *sneak into basket pattern*, see for instance C. II. 1.c) below.

70 See C. II. 2. a) and C. II. 2. c) below.

This once again highlights a serious issue when analysing “dark patterns”. Difficult definitions, the existence of a constantly evolving actual setting and an inconsistent understanding of the phenomenon already make it difficult to categorise individual examples. For this reason, the relevance of “dark patterns” in individual sectors is even more difficult to determine empirically.

C. Legal assessment[71]

Based on these facts, a legal analysis will be carried out below to answer the question of whether and which legal reforms are necessary to deal with "dark patterns".

1. What role does consumer sovereignty and the balancing of fundamental rights play in the development of Consumer Law?
2. What requirements must be met by the factual basis and its proof to justify legislative projects?
3. How can sector-specific law be created without the risk of fragmentation of the legal framework?
4. Which regulations already apply to the practices?
5. If regulatory and enforcement gaps exist: How can these be closed in a considerate manner?

I. Fundamental rights framework for the regulation of "dark patterns"

Before analysing which legal requirements exist regarding the digital environment and "dark patterns" and in which areas there may be gaps in enforcement, it necessary to show which framework conditions exist through fundamental rights requirements in order to counter "dark patterns".

1. Juxtaposition of different fundamental rights and principles

a) Consumer protection, the modern consumer model and consumer sovereignty, Art. 12, 169 TFEU, Art. 38 CFR

Ensuring a high level of consumer protection in EU Primary Law follows from Art. 12, 169 TFEU[72] and subsequently, from a fundamental rights perspective, from Art. 38 CFR[73]. However, the requirements of Primary Law do not specify the necessary level of consumer protection in more detail and leave the legislators extensive room for manoeuvre.[74] The shaping of consumer protection provisions and the establishment of a consumer model on the basis of which new provisions are to be created is therefore not predetermined in detail by fundamental rights, but is largely left

---

71 This examination is based in part on a legal opinion by the authors: *Kühling/Sauerborn*, Rechtsgutachten über die rechtlichen Rahmenbedingungen sogenannter "dark patterns", available at: https://bevh.org/fileadmin/content/04_politik/Europa/Kuehling-Gutachten-BEVH-Dark-pattern-22-02-16-final.pdf.

72 Treaty on the Functioning of the European Union.

73 Charter of Fundamental Rights of the European Union.

74 See *Jarass*, in: Jarass (ed.), Commentary on the CFR, 2021, Art. 38 para. 9.

to the Union and its Member States. Nevertheless, a five-pole protection concept follows from Art. 38 CFR. In addition to the supply of goods and services to consumers, pricing must be guaranteed. Furthermore, the physical integrity and also the personal integrity of the consumer must be protected, whereby the latter must be ensured in EU Primary Law in particular by the data protection provisions in Art. 8 CFR and Art. 16 TFEU. Finally, the protection of consumer's interests, i.e. the protection of the consumer's economic and immaterial preferences, must be ensured.[75]

Art. 38 CFR functions as a so-called principle within the meaning of Art. 52 (5) CFR and therefore does not have the function of a fundamental right and does not give consumers, consumer associations or representative bodies the right to enact protective measures or specific arrangements.[76] Nevertheless, principles must be implemented through legislative acts, Art. 52 (5) 1 CFR.

For the legislator to implement these principles, it must have some idea of how the consumer is to be defined in order to determine the level of protection to be achieved.[77] Furthermore, standardisation is also necessary when interpreting consumer protection standards in order to be able to fill in the content of undefined legal terms.[78] The currently prevailing so-called "modern consumer model" results from the need for standardisation. This has been characterised in particular by the interpretation of Primary and Secondary Union Law by the ECJ[79] and has also found its way into legislation.[80] When determining the standard of protection of consumer protection provisions, the ECJ assumes that the average consumer is reasonably well informed and reasonably observant and circumspect.[81] In particular, this is intended to ensure a balance between entrepreneurial freedom on the one hand and the risk of consumers being misled on the other. Furthermore, the ECJ also refers to the criterion of proportionality in connection with interventions in the freedom to conduct

---

75 *Schmidt-Kessel*, in: Pechstein/Nowak/Häde (eds.), Frankfurt Commentary on the TEU, CFR and TFEU, 2023, Art. 38 CFR, para. 25.

76 *Schmidt-Kessel*, in: Pechstein/Nowak/Häde, Frankfurt Commentary on the TEU, CFR and TFEU, 2023, Art. 38 CFR, para. 5.

77 *Alexander*, in: Gsell/Krüger/Lorenz/Reymann (eds.), Beck Online Great Commentary, status 2024, Section 13 of the German Civil Code (BGB), para. 385.1 with further references.

78 For example, the term "unfair" in the general clause of Art. 5 (2) UCPD.

79 European Court of Justice.

80 See Recital 18 of the UCPD: "the average consumer [...] who is reasonably well-informed and reasonably observant and circumspect [...]".

81 *ECJ*, judgement of 16/7/1998, C-210/96 – *Gut Springenheide*, para. 31; *ECJ*, judgement of 28/1/1999 – C-303/97 – *Sektkellerei Kessler; ECJ*, judgement of 4/5/1999 – *Windsurfing Chiemsee*; *ECJ*, judgement of 22/6/1999 – *Lloyds/Loints*.

a business, which should be safeguarded by a corresponding consumer model.[82] The consumer model therefore plays an important role in determining the necessary level of consumer protection.

By choosing the modern consumer model, the legislator has opted for a middle way between paternalism and an economically liberal approach. The modern consumer model does not take the consumer by the hand in such a way that he or she must be protected from any influence, but instead opts for a certain degree of responsibility. However, no above-average prerequisites are placed on the consumer's attentiveness and intellect.

On the other hand, case law attempts to counter the risk of under-protection of under-informed, under-attentive or unreasonable consumers arising from this modern consumer model by focussing on the specific target group orientation of offers,[83] and the circumstances of the individual case.[84] As a result, expectations of consumers are lowered when business models are geared towards certain consumer groups. In these cases, it is no longer the general average consumer but the average consumer of the respective group that is decisive.[85]

Whether the modern consumer model can also be applied to modern, digitally driven business practices in particular has recently been the subject of controversial debate. Case law trends,[86] which once again place greater emphasis on protecting the consumer, are fuelling this discussion. There are concerns as to whether the consumer, as assumed with the modern consumer model, can still meet those market players on an equal footing. In particular, the modern consumer model is said to not being applied if the information available to the consumer is predetermined on the internet, meaning that the consumer would not be adequately informed. *BEUC* also points out that

---

82 *ECJ*, judgement of. 13/1/2000 – C-220/98 – *Lifting-Crème*, para. 27, 28; see also *Köhler*, in: Köhler/Bornkamm/Feddersen (eds.), Commentary on the German Unfair Competition Act (UWG), 2024, Section 1 UWG para. 22.

83 *ECJ*, judgement of. 13/1/2000 - C-220/98 – *Lifting-Crème*, para. 29; *ECJ*, judgement of 6/5/2003 – C-104/01 – *Libertel*, para. 46; *ECJ*, judgement of 4/6/2015 – C-195/14 – *Himbeer-Vanille-Abenteuer*, paras. 36-42.

84 *ECJ*, judgement of 13/1/2000 – C-220/98 – *Lifting-Crème*, para. 30; see also *Köhler*, in: Köhler/Bornkamm/Feddersen (eds.), 2024, Section 1 para. 25.

85 See Recital 18 UCPD: "[...] also contains provisions aimed at preventing the exploitation of consumers whose characteristics make them particularly vulnerable to unfair commercial practices. Where a commercial practice is specifically aimed at a particular group of consumers, such as children, it is desirable that the impact of the commercial practice be assessed from the perspective of the average member of that group. It is therefore appropriate to include in the list of practices which are in all circumstances unfair a provision which, without imposing an outright ban on advertising directed at children, protects them from direct exhortations to purchase.".

86 *ECJ*, judgement of 18/10/2012 – C-428/11 – *Purely Creative*.

asymmetries would exist in the digital sector, which would argue in favour of granting the consumer a lower level of responsibility in order to restore a balance.[87] The same should apply if the consumer is tempted to take an action desired by the trader due to increased obstacles to other alternative actions, such as lock-in effects in particular.[88]

The consumer model is handled dynamically and is adapted to the respective situations, be it due to the specific characteristics of consumers or companies. In principle, the modern consumer model is applied. In terms of business models, however, there are already tendencies to assume a greater need for protection. This would also be conceivable for the constellation that a company uses "dark patterns", provided that this would result in a special need for protection of the consumer. However, it should also be noted that businesses, also those which use "dark patterns", are themselves protected by fundamental rights. The ECJ has developed the modern consumer model precisely against the background of the proportionality of interventions in entrepreneurial freedom.[89] This will have to be taken into account when standardising and interpreting norms that regulate "dark patterns".

Finally, the concept of consumer sovereignty must be discussed in connection with the modern consumer model. This discussion takes place in particular in connection with the UCPD, which is designed to also ensure consumer sovereignty. The aim of the UCPD is that consumers must be able to make their decisions based on the value for money and quality of the goods or services offered. It is therefore to safeguard the sovereignty and rationality of consumers' decisions against the dangers posed by a lack of transparency of offers, pressure to buy or deceptive or misleading advertising.[90] This demonstrates the idea of consumer sovereignty as follows: Sovereignty does not imply a statutory, paternalistic predetermination of what is good or bad for the consumer. Such paternalism would not be compatible with the concept of consumer sovereignty. In contrast, the legislator must ensure that the consumer achieves an environment in which he or she can fulfil their own wishes and needs without unfair constraints and non-transparent or misleading designs. The legislator must take this into account when creating new provisions.

---

87 *BEUC*, "Dark Patterns" and the EU Consumer Law Acquis, p. 9, available at: https://www.beuc.eu/sites/default/files/publications/beuc-x-2022-013_dark_patters_paper.pdf.

88 See *Podszun*, in: Harte-Bavendamm/Hennig-Bodewig (eds.), 5th ed. 2021, Section 1 UWG paras. 55-56a with further references.

89 On entrepreneurial freedom, see b) below.

90 Summarising the German implementation of the UCPD: *Nassal*, NJW 2006, 127, 129. On the parallel discussion of consumer sovereignty in Competition Law *Crémer/de Montjoye/Schweitzer*, Competition Policy for the digital era, 2019, p. 77.

b) Entrepreneurial freedom, Art. 16 CFR

Entrepreneurial freedom is explicitly codified in Article 16 CFR, which opens up the personal scope of protection for the operators of a company. Operators can be both natural and legal persons,[91] but also associations of persons[92]. In substantive terms, the scope of protection is opened up for entrepreneurial activities, whereby this term is to be interpreted broadly and only requires that the activity is permanent, independent and profit oriented, regardless of whether the company is also an employer.[93] This protects the freedom of a company to pursue an economic or business activity,[94] and includes a wide range of specific protections, from the establishment of a company, the organisation of the business and its recruitment to the free use of resources and freedom of trade. Art. 16 CFR also protects the freedom of contract of companies, which includes the freedom to choose the contracting parties and the content of the contract, including the subject matter of the contract and pricing. In addition, entrepreneurial freedom protects the freedom to advertise, meaning that the freedom to conduct a business can be supplemented by the freedom of communication under Art. 11 (1) CFR.[95] This means that the design of a company's presence vis-à-vis consumers enjoys special protection under fundamental rights. There are some arguments in favour of granting website operators increased protection under fundamental rights when choosing the design of their website, including its user interfaces, supplemented by the freedom of communication under Art. 11 (1) CFR, since website operators generally communicate with customers almost exclusively via their website. This is why the design of the website and the possibilities for interaction with the consumer are decisive for the customer's perception of the company. The design therefore has a direct advertising effect.

Art. 16 CFR is given a special dimension of protection in that the entrepreneurial freedom adds a subjective-legal dimension of protection to the objective-legal principle of competition in the European Union, so that companies have a right to participate in undistorted competition.[96]

---

91 *Kühling/Drechsler*, in: Pechstein/Nowak/Häde (eds.), 2023, Art. 16 CFR, para. 5.
92 Clarifying: *Jarass*, in: Jarass, 2021, Art. 16 CFR, para. 12.
93 *Kühling/Drechsler*, in: Pechstein/Nowak/Häde (eds.), 2023, Art. 16 CFR, para. 13 with further references.
94 See *ECJ*, judgement of 22/1/2023 – C-283/11 – *Sky Austria,* para. 42.
95 Comprehensively *Kühling/Drechser*, in: Pechstein/Nowak/Häde (eds.), 2023, Art. 16 CFR, para. 14 with further references; see also *ECJ*, judgement of 17/12/2015 – C-157/14 – *Neptune Distribution SNC*.
96 *Kühling/Drechsler*, in: Pechstein/Nowak/Häde (eds.), 2023, Art. 16 CFR, para. 17.

Due to regulatory approaches under Union Law such as in Competition Law, Company Law and Contract Law, interventions in entrepreneurial freedom, which cover both direct and indirect interventions, are many and varied. Nevertheless, decisions of the ECJ in which Art. 16 CFR plays a role are rare.[97] This may be due to the principle of normative referral enshrined in EU Procedural Law, which means that the ECJ only examines the fundamental rights to which the parties refer in their submissions. For example, in the Google Spain decision[98] on the obligation of search engine operators to delete personal data, the ECJ did not address possible violations of the entrepreneurial freedom, although such an examination would have been worthwhile.[99] A recurring group of cases that justifies strict interventions in entrepreneurial freedom in the case law of the ECJ[100] is consumer protection, which must be objectively guaranteed in accordance with Art. 38 CFR.[101]

This also reveals a multi-dimensional protective effect that must be taken into account when regulating "dark patterns" – both when interpreting existing and creating new provisions. On the one hand, entrepreneurial freedom protects, among other things, business models, i.e. the way in which a company generates value. In addition, entrepreneurial freedom also protects the free organisation of contracts and the choice of contractual partners. This means that business activities that contain elements of "dark patterns" are also protected in principle if they are used for commercial gain. On the other hand, the entrepreneurial freedom of competing market players gives rise to a right to legally undistorted competition. This is addressed in particular by the UCPD, which provides for protection of fair competition in addition to the protection of consumers. Restrictions on the use of "dark patterns" can therefore result not only from the obligation to ensure consumer protection, but also directly from the obligation to ensure undistorted competition resulting from entrepreneurial freedom.

97 See *Kühling/Drechsler*, in: Pechstein/Nowak/Häde (eds.), 2023, Art. 16 CFR, para. 22 and footnote 111.
98 *ECJ*, judgement of 13/05/2014, C-131/12 – Google Spain.
99 *Kühling/Drechsler*, in: Pechstein/Nowak/Häde, 2023, Art. 16 CFR para. 26.
100 *ECJ*, judgement of 17/12/2015, C-157/14 – *Neptune Distribution SNC*, paras. 72 et seq. See also *ECJ*, judgement of 30/6/2016, C-134/15 – *Lidl*, paras. 35 et seq.
101 See a) above.

c) Right to data protection, Art. 7, 8 CFR

In the area of data processing and, in particular, personalisation, the right to privacy and data protection under Art. 7, 8 CFR are relevant. The ECJ applies both fundamental data protection rights from Art. 7 and 8 CFR largely in parallel. [102]

In addition to its function as a classic right of defence for citizens against state interference, the fundamental right to data protection generates a comprehensive duty of protection for public authorities, which must be ensured in particular by statutory regulations for data processing bodies - including private ones.[103] The scope of protection is extremely broad – all personal data, i.e. all information about a specific and identifiable or identified or identifiable natural person, is protected. Any kind of personal data is protected, regardless of how dangerous its processing or disclosure is.[104] The processing of personal data, as it is to be understood in the sense of the secondary legislation enacted, constitutes an interference. Processing is the generic term for all data processing steps, from collection to disclosure to erasure.[105] Personal data must be processed *fairly* for specified purposes and is subject to consent or another legitimate basis regulated by law in accordance with Art. 8 (2) 1 CFR. Consent can only justify an interference with fundamental rights if it is sufficiently informed and voluntary. The implementation of the fundamental right to data protection, in particular in the GDPR[106], is important in this context.

d) Interim result

The legislation that is supposed to deal with "dark patterns" is subject to a legal framework which, on the one hand, requires a high level of consumer protection, consumer sovereignty and data protection, but on the other hand, prohibitions also mean interference with the entrepreneurial freedom and, where applicable, the freedom of communication of traders. Each of the fundamental rights or principles can therefore not stand alone and serve as an end in itself. There is also no hierarchy of rights. The legislator must therefore skilfully balance the conflicting and various positions. Therefore, the creation of prohibitions must be skilfully handled, and the relevant rights and interests of all parties involved must be protected.

---

102 See *ECJ*, Opinion 1/15 of 26/7/2017, – *PNR Agreement with Canada,* para. 140; see also *Kühling/Klar/Sackmann*, Data Protection Law, 2021, paras. 44 et seq.

103 *Kühling*, in: Pechstein/Nowak/Häde (eds.), 2023, Art. 8 CFR, para. 10.

104 *Kühling*, in: Pechstein/Nowak/Häde (eds.), 2023, Art. 8 CFR, paras. 14 et seq.

105 *Kühling/Klar/Sackmann*, Data Protection Law, 2021, paras. 50 et seq.

106 General Data Protection Regulation 2016/679.

2. Requirements by the factual basis to justify legislative projects

This in turn raises the question of what proof is required of the legislator if it wishes to prohibit specific practices. As has been shown, the area of "dark patterns" is characterised by a complex regulatory framework of fundamental rights that need to be balanced.

As shown, prohibitions of practices by companies constitute interference with their entrepreneurial freedom under Art. 16 CFR. However, the case law of the ECJ generally allows for significant interventions to create a high level of Consumer Law.[107]

On the other hand, although the investigations by the EU Commission and the CPC network found in their view a large number of cases of "dark patterns", these are, at least in the study assigned by the EU Commission, in some parts not attributable to the sector of online retail and B2C marketplaces. In addition, as shown, there are also practices that do not clearly constitute "dark patterns", as the term was understood very broadly in the investigation.

Against the background of necessity, the principle applies that the more far-reaching the interference, the more likely it is to require objective justification on a factual basis. However, to date, the ECJ has tended to grant the legislator a wide margin of manoeuvre in complex economic situations and only object to manifestly disproportionate interventions in entrepreneurial freedom.[108] Nevertheless, this should be viewed critically, as it effectively places the burden of proof on the subject of fundamental rights to demonstrate that a measure is not necessary.[109]

With the correct interpretation, it therefore follows that in the case of encroachments on entrepreneurial freedom, the legislator must provide evidence of the necessity of a measure depending on the severity of the encroachment on fundamental rights. This means that greater proof is required when prohibitions encroach particularly far-reaching on entrepreneurial freedom. Conversely, the smaller the encroachment, the less justification is required on a factual basis. However, it is not only the severity of the interference per se that must be taken into account – the more the interference is intended to prohibit an entire business model, for example, and therefore the closer it comes to the essence of the fundamental right[110], the higher the requirements. The incurrence of higher

---

107 *ECJ*, judgement of. 17/12/2015, C-157/14 – *Neptune Distribution SNC*, paras. 72 et seq. *ECJ*, judgement of 30/6/2016, C-134/15 – *Lidl,* paras. 35 et seq.

108 See for example *ECJ*, judgement of. 17/10/2013, C-101/12 – *Schaible*, para. 48; ECJ, judgement of 4/5/2016, C-477/14 – *Pillbox 38*, para. 49; ECJ, judgement of 28/3/2017, C-72/15 – *Rosneft*, para. 146; ECJ, judgement of 2/9/2021, C-570/19 – *Irish Ferries*, para. 151.

109 *Kühling/Drechsler*, in: Pechstein/Nowak/Häde (eds.), 2023, Art. 16 CFR, para. 22.

110 On the term *Kühling/Drechsler*, Pechstein/Nowak/Häde (eds.), 2023, Art. 16 CFR, para. 20.

compliance costs due to ensuring compliance is also relevant in this context, as this also constitutes an intervention. Against this background, a lot speaks in favour of the necessity of further evidence of practices worthy of prohibition to justify tightening rules regarding "dark patterns".

3. The relationship between the creation of sector-specific law and the risk of fragmentation

In connection with the proportionality of interventions in entrepreneurial, the question also arises as to how fragmented a regulatory regime may be. A large number of "dark patterns" only occur in specific sectors. For example according to the studies, *address book leeching* does not occur at all in the online retail and online B2C marketplace sector.

Fine-meshed, sector-specific regulation has the advantage that it only burdens those subjects of fundamental rights where certain practices actually occur. On the other hand, sector-specific regulation that is too fine-meshed can lead to a high degree of fragmentation, which makes it more difficult to apply the law against the background of comprehensible regulations.[111] As can already be seen from a large number of recent digital legislation in the EU, this is certainly problematic, as the partially overlapping regulations with sometimes unclear boundaries lead to increased legal uncertainty which is further complicated by different interpretations of the provisions by the Member States.[112]

A compromise must therefore be found that both prevents "collateral damage" through overly broad regulation, but at the same time is not so finely meshed that the application of law is made too difficult. However, it should be pointed out in this context that previous regulations on "dark patterns" in EU legislation already show sector-specificity within a regulatory framework, which has not detracted from transparency. For example, there are demarcations between general Consumer Contract Law and special distance selling contracts that have not led to any unclear overlaps between the addressees and thus to legal uncertainty. It is likely that this is because the provisions are largely contained within one and the same set of rules, so that they have been harmonised by the same responsible parties, which may have prevented subsequent demarcation problems.

111 See *Kingreen/Kühling*, Juristenzeitung (JZ) 2015, 213, on the problem that is being discussed in Germany against the background of the clarity and certainty of standards, on the (overly) complex former regulatory structure in Social Data Protection Law.

112 One example of this is the demarcation between the ePrivacy Directive and the GDPR in Art. 95, which has led to great legal uncertainty in the area of data protection in electronic communications in Germany, for example, for years and continues to do so. See *Kühling/Sauerborn*, Computer und Recht (CR) 2021, 271 on this and more recent developments. *Bomhard*, MMR 2024, 71, 73 et seq. on the interplay between the Data Act and the GDPR.

Against this background, it seems advisable that, should new rules be created, these are not implemented in numerous individual acts that are applicable in parallel (such as a new "Digital Fairness Act" being applicable besides the UCPD), but as amendments in already existing acts (such as the UCPD), and then be divided up within these laws on a sector-specific basis.

II. Analysis of the current regulations on "dark patterns"

Having elaborated which conditions in Fundamental Law exist for the creation and interpretation of provisions on "dark patterns" and which standards must be met when establishing new provisions, it is now necessary to examine how the current regulatory regime addresses "dark patterns".

1. Regulations in Consumer Contract Law

As a large proportion of "dark patterns" are aimed at business transactions unwanted or disadvantageous for the consumer, it is first examined whether Consumer Contract Law provides sufficient protection for the contractual partner against such practices. The CRD and the UCTD were decisive for the provisions of Consumer Contract Law.

a) Development of the provisions

Current Consumer Contract Law in the member states of the Union is strongly characterised by Union Law and is by no means based solely on current provisions. For example, special rules on contracts concluded away from business premises were already laid down in 1985 and provisions on distance selling contracts in 1997. The CRD, being implemented in 2011, was then intended to develop a uniform standard of Consumer Law[113], which in particular addressed the modern consumer model.[114] Nevertheless, most of the provisions contained therein were not new at the time. In particular, the provisions continue to focus on contracts negotiated away from business premises and distance selling contracts. The provisions on general Consumer Protection Law are supplemented by other sector-specific provisions, such as the Digital Content Directive[115] and the Sale of Goods Directive,[116] which had to be implemented in the provisions of the member states in 2022 through new and reformed provisions. Consumer Contract Law regulations reflect the modern consumer model and the so-called "information model", which has a significant influence on internal market legislation.[117] The information model is based on the idea that market players can adequately realise their market opportunities through sufficient information and that competition between traders is fundamentally sufficient to ensure a fundamentally advantageous market for all

113 The directive was therefore adopted as a fully harmonising directive, see Art. 4 CRD.
114 See I. 1. a) above.
115 Directive 2019/770.
116 Directive 2019/771.
117 See *Ackermann*, Zeitschrift für Europäisches Privatrecht (ZEuP) 2009, 230.

market participants. Only where there is a market failure should substantive measures be taken.[118] For example, the Consumer Rights Directive is primarily based on obligations to provide the consumer with comprehensive information so that they can make a rational purchase decision.[119] In addition to these comprehensive information obligations, Consumer Contract Law provides consumers with a right of cancellation for many situations so that they can withdraw from contracts without having to overcome major hurdles.[120] In this way, Consumer Contract Law also deals with practices that fall under "dark patterns" and are based on false or concealed information provided to the consumer.

b) Comprehensive information obligations in Consumer Contract Law, Art. 5 CRD

Consumer Contract Law contains detailed information obligations. General information requirements for consumer contracts can be found in Art. 5 CRD. They contain information on the essential characteristics of the goods or services, including the identity of the trader, the total price of the goods and services including all taxes and duties or the method of price calculation, more detailed terms of payment, delivery and performance, the statutory rights arising from liability for defects and guarantees or after-sales services, contract terms, conditions for cancellation and automatic renewals and the functioning of digital content and, where applicable, restrictions on interoperability and compatibility with hardware and software. Extended information obligations can also be found for distance and off-premises contracts in Art. 6 CRD, which extends the scope of the necessary information to deal with special constellations. Finally, further information obligations arise from Art. 10 et seq. E-Commerce Directive[121] for contracts in electronic commerce, which represent a special case of distance contracts. The corresponding information obligations from the CRD therefore remain in place and are supplemented by electronic commerce-specific information obligations, for example on the technical steps leading to the conclusion of the contract. What the information obligations have in common is that they contain regulations on the transparency of the information. For example, the information must be provided "in a clear and comprehensible manner"[122] or "clearly, comprehensibly and unambiguously"[123].

---

118 For more details on the above, see *Hacker*, Verhaltensökonomik und Normativität, 2017, p. 395 et seq. and on Consumer Contract Law in particular p. 402 et seq.

119 See the headings of Chapters II and III of the CRD, which focus on consumer information.

120 Art. 9 CRD.

121 Directive 2000/31/EC.

122 Art. 5 et seq. CRD.

123 Art. 10 E-Commerce Directive.

If the provisions and their national implementations are interpreted accordingly, such practices are prohibited in Consumer Contract Law that are based on the omission or concealment of material information or its analysability when concluding a contract, such as *hidden information*, *hidden costs, trick questions, bait and switch* or *misdirection* patterns.

c) Prohibition of default settings, Art. 22 CRD

Art. 22 CRD contains a ban on "hidden" ancillary services, in that such services may only be expressly agreed. Examples of this are pre-ticked boxes for additional insurance policies or clauses in general terms and conditions in which additional services subject to a fee are agreed. The provision applies to all consumer contracts. This prohibits all practices in the area of Consumer Contract Law that are based on foisting unwanted additional services on the consumer, such as *preselection* and *sneak-into-basket* patterns.

d) Special transparency provisions and button solution in the e-commerce sector, Art. 8 (2), (3) CRD

In the area of electronic commerce, there are also increased transparency requirements in Art. 8 (2) and (3) CRD. For example, the trader must provide the consumer with essential information, namely the essential characteristics of the goods or services, the total price, in the case of open-ended contracts or subscription contracts the billing period and the contract term or cancellation conditions and the minimum duration of the obligations entered into in a "clearly and in a prominent manner, and directly before the consumer places his order". This is intended to present the essential information of the contract clearly and unambiguously to the consumer before concluding the contract. If, due to the large amount of information or a smaller screen, such as that of a smartphone, scrolling is necessary to view the entire information in full, with a correct understanding of the provision, the order button should only be displayed once the consumer had the opportunity to view all the information.[124]

In addition, the "button solution" is also covered in Art. 8 (2) (2) CRD. The trade has to design the button for concluding the contract in such a way that only the words „order with obligation to pay" or a clear corresponding formulation are displayed in a legible manner. This is therefore a special

[124] *Wendehorst*, in: Säcker/Rixecker/Oetker/Limperg (eds.), Munich Commentary on the German Civil Code, 2022, Section 312j para. 17; Regional Court of Berlin, judgement of 17/7/2013 – 97 O 5/13, paras. 13 et seq.

transparency provision It makes it clear that the order button itself may not contain any other information in addition to the conclusion of the contract that might distract from the order requiring payment. The strictness with which this must be handled was confirmed in Germany by the Kammergericht Berlin (KG)[125] in a decision[126] in which it was determined that the wording "Start membership – chargeable after free month"[127] on the button does not fulfil the requirements. In addition to the wording of Section 312j of the German Civil Code[128], which implements the button solution in German Law, this was also justified by the fact that the wording "free month" distracts from the fact that the offer is subject to a charge and the button therefore does not sufficiently fulfil its warning function.[129] The button solution thus prevents unexpected contract conclusions in Consumer Contract Law in electronic legal transactions. In particular, this addresses *bait-and-switch, misdirection* and *forced continuity* patterns.

e) Cancellation rights, Art. 16 CRD

Another instrument that consumers have at their disposal to eliminate any unwanted contracts simply and without further conditions are cancellation rights for distance and contracts negotiated away from business premises in Art. 16 CRD.[130] The statutory cancellation right fulfils a dual function: on the one hand, it addresses a problem that is also exploited by "dark patterns", namely short-term and imprudent decisions due to a surprising situation, as is assumed in the case of contracts negotiated away from business premises.[131] This idea is particularly useful in the case of information asymmetries, as can be the case with "dark patterns". However, they are also intended to compensate for the consumer's lack of information in distance selling contracts, which is in the essence of the matter if, unlike in a shop, the consumer cannot pick up the goods and examine their functionality or properties.[132]

This provides the consumer with a powerful tool to remedy the consequences of hasty concluded contracts at low cost, which in many cases prevents *roach motel* patterns. However, in order to protect the trader, the legislator attempts to counter the unilateral possibility of cancelling contracts

125 Higher Regional Court of in Berlin.
126 KG Berlin, judgement of. 20/12/2019 – 5 U 24/19.
127 In the original: "Mitgliedschaft beginnen – kostenpflichtig nach Gratismonat".
128 Bürgerliches Gesetzbuch, BGB.
129 See also *Martini/Drews/Seeliger/Weinzierl*, ZfDR 2021, 47, 60.
130 For the cancellation button, see III. 2. b) iii. below.
131 See, for example, *ECJ*, judgement of 7/8/2018 – C-485/17, para. 33 – *Unimatic*.
132 Recital 14 of the Distance Contracts Directive 97/7/EC.

in unreasonable cases by regulating numerous exceptions to the right of withdrawal in Art. 16 CRD. In doing so, the legislator is partly countering the situation of so-called *moral hazard* that easily arises with cancellation rights, i.e. the situation in which one party can act unfairly to the detriment of the other party without being observed and without sufficient compensation.[133] For example, there is no right of cancellation from the outset for individually manufactured and perishable goods, as the trader could no longer use the items after exercising the right of cancellation. In addition, the consumer subsequently loses the right of cancellation if the goods have been inseparably mixed with other goods, if sealed packaging of sound storage media or software has been opened or in the case of magazines. Here, the legislator assumes that it would be unfair to grant the consumer a right of cancellation if the goods may have already fulfilled their function. Further exceptions can be found in the provision of services and digital content which is not supplied on a tangible medium if the trader has provided the service or started to fulfil the contract and the consumer has previously expressly consented to the loss of the right of withdrawal.

f) Transparency obligations under the new provisions on the Sale of Goods

New transparency obligations were recently created in Consumer Contract Law with the Sale of Goods Directive. Indirectly, the equal treatment of objective and subjective characteristics of goods in terms of conformity with the contract or their lack of conformity in Art. 6 et seq. of the Sale of Goods Directive in combination with formal requirements for agreements on the deviation of objective characteristics of goods in the area of the sale of consumer goods (Art. 21 of the Sale of Goods Directive) leads to very comprehensive information obligations on the part of the trader regarding the characteristics of the goods. Due to the equal importance of subjective and objective expectations of the quality of the goods, the individual buyer's expectations are no longer relevant. In the area of the sale of consumer goods, which is particularly relevant for the sector of online retail, deviations from the objective expectation in the form of quality agreements are also subject to formal requirements, which means that the consumer must be comprehensively informed about the characteristics of the goods, even if he or she already knows the object of their purchase. Since Art. 7 (5) of the Sale of Goods Directive subjects the waiver of the objective requirements for lack

[133] The right of cancellation not only eliminates contracts that were concluded on the basis of short-term decisions or a lack of information. Rather, there are numerous cases in which the right of cancellation is used contrary to its actual purpose in order to order "for selection", i.e. with the already established intention of a (still undetermined) return. *Hacker*, Verhaltensökonomik und Normativität, 2017, p. 521 et seq., correctly pointing out this risk and with further references.

of conformity to special requirements, the trader cannot rely on the buyer's knowledge or grossly negligent lack of knowledge if the information is omitted.[134]

The fact that this obligation to provide information is intended to counteract the fuelling of heightened consumer expectations, as is sometimes exploited by "dark patterns" in the offline world, is particularly evident in the provision that samples and specimens made available to the consumer before the purchase can form the standard for the objective conformity of the goods with the contract, Art. 7 (1) lit. b of the Sale of Goods Directive. This means that the consumer must expressly and formally agree to characteristics of the goods that deviate from the samples and specimens in the form of a quality agreement.[135]

g) Interim result

The regulations in Consumer Contract Law already provide effective mechanisms against many categories of "dark patterns". In addition to comprehensive information obligations and button design as well as the ban on *preselection*, there are easy-to-exercise cancellation rights that can eliminate the consequences of contract conclusions based on manipulation.

De lege lata, there are therefore precise provisions in Consumer Contract Law that can address a large number of known categories of "dark patterns" or at least eliminate their undesirable consequences in a cost-effective manner. This shows that the European legislator is constantly adapting Consumer Contract Law to new circumstances as a result of new business models with new undesirably influencing practices in fine detail, even with the modern consumer model in mind, and prohibiting new groups of cases of influence if these are categorically unacceptable.

A need for legislative action that specifically addresses and prohibits "dark patterns" is therefore not triggered in Consumer Contract Law. Of course, Consumer Contract Law mechanisms are dependent on the use by consumers taking legal actions. It therefore seems conceivable that the consumer will accept the contractual consequences in individual cases if the risk of legal proceedings is higher than the benefit of cancelling or rescinding the unwanted contract. This is conceivable in cases in which "dark patterns" lead to undesirable but relatively unencumbering contracts. Traders could thus be inclined to conclude a large number of contracts while using "dark patterns", but at the same time keep the impact on the individual low so that they will not take legal actions. These

134 *Faust*, in: Hau/Poseck (eds.), Beck Online Commentary, German Civil Code, 2023, Section 475 para. 31.
135 Comprehensively on this: *Lorenz*, Neue Juristische Wochenschrift (NJW) 2021, 2065, 2072, 2073.

problems cannot therefore be solved by substantive law alone, but also require additional institutional support in Consumer Protection Law, as provided for by the UCPD.

2. The Unfair Commercial Practices Directive

The UCPD also contains rules that address "dark patterns". This area, which aims to protect consumers from "unfair business-to-consumer commercial practices" as a general preventative measure[136] focuses on "transactional decisions"[137] by consumers. It therefore protects the consumer's freedom of choice as their autonomous control in commercial transactions" before, during and after a commercial transaction"[138].[139]

This is to be achieved by providing consumers with all the information they need "depending on the circumstances, in order to make an informed commercial decision".[140] In the UCPD, this is carried out by prohibiting actions that influence the consumer's will beyond what is permissible.[141] This clearly shows that the UCPD, as well as Consumer Contract Law, is based on the modern consumer model of the average informed and attentive consumer.[142]

The scope of application in the UCPD is extremely broad and includes "commercial practices". According to Art. 2 lit. d UCPD, such practices are "act, omission, course of conduct or representation, commercial communication including advertising and marketing, by a trader, directly connected with the promotion, sale or supply of a product to consumers". A product is defined as "any good or service including immovable property, digital service and digital content, as well as rights and obligations"[143]. This means that a commercial practice exists if it is company- and market-related. Examples include the conclusion of contracts, advertising to promote sales and facts relevant to Data Protection Law as long as they are market-related, such as measuring the reach of advertising.[144] This also becomes clear in the definition of the transactional decision,[145] which is

136 See Art. 3 (1) UCPD.
137 Art. 2 lit. k UCPD.
138 Art. 3 (1) UCPD.
139 *Sosnitza*, in: Heermann/Schlingloff (eds.), Munich Commentary on the German Unfair Competition Act (UWG), 2020, Section 1 para. 27.
140 Art. 7 (1) UCPD.
141 See *Köhler*, in: Köhler/Bornkamm/Feddersen (eds.), 2024, Section 1 para. 19.
142 See I. 1. a) above.
143 Art. 2 lit. d UCPD.
144 See *Keller*, in: Harte-Bavendamm/Henning-Bodewig (eds.), Section 2, para. 31a.
145 Art. 2 lit. k) UCPD.

the starting point for materially distorting the economic behaviour of consumers[146] prohibited under Art. 5 (2) UCPD. The term is also very broad and covers any decision by a consumer on whether, how and under what conditions to buy, pay for, keep or dispose of a product in whole or in part, or to exercise a contractual right in relation to the product, regardless of whether the consumer decides to take or refrain from taking an action. The UCPD thus also proves its worth in newer business models, such as social networks or platforms, as it does not require any direct monetary consideration in order to qualify an action as commercial practice. Concerns that newer business models would not be covered by the UCPD due to an alleged paradigm shift are therefore unfounded.[147] With a correspondingly broad interpretation of the term, it also seems superfluous to introduce a further term of "digitally unfair commercial practices". There is much to suggest that this would lead to further difficulties to define such practices and distinguish them from general commercial practices, whereby a correct interpretation of the term would mean that all forms of consumer influence would already fall under the general term.[148]

a) Generally unauthorised acts according to Annex I UCPD

The practices directed at consumers on the list in Annex I of the UCPD are always considered unfair "without a case-by-case assessment"[149]. It is therefore not necessary to examine unfairness according to the offences in Art. 5 to 9 UCPD. Annex I prohibits a number of practices that can also be characterised as "dark patterns".

Firstly, this concerns No. 7 of Annex I, which prohibits an untrue temporal *scarcity* or time-limited offer conditions of goods or services if this is intended to induce the consumer to make an immediate decision without having time to decide on the basis of sufficient information.[150] The time period must be so limited that the consumer feels under great pressure to make a decision. This

146 Art. 2 lit. e) UCPD.

147 In that sense *Helberger, Kas, Micklitz, Namyslowska, Naudts, Rott, Sax, Veale*, Digital Fairness for Consumers, 2024, available at: https://pure.eur.nl/ws/portalfiles/portal/139212255/BEUC-X-2024-032_Digital_fairness_for_consumers_Report.pdf, p. 193-196, 216. However, as already indicated there, the question as to whether there is a charge can be resolved by interpretation. For example, there are many arguments in favour of also classifying mechanisms of personalisatzion or additive design as commercial practices, as they are at least indirectly related to the sales promotion.

148 But this way *Helberger, Kas, Micklitz, Namyslowska, Naudts, Rott, Sax, Veale*, Digital Fairness for Consumers, 2024, available at: https://pure.eur.nl/ws/portalfiles/portal/139212255/BEUC-X-2024-032_Digital_fairness_for_consumers_Report.pdf, p. 216 et seq.

149 Recital 17 of the UCPD.

150 For another *scarcity* pattern, that of limited availability, see c) below.

addresses those "dark patterns" that are intended to put the consumer under time pressure, for example a *countdown* pattern such as "this offer ends in 10 minutes". However, it is subject to two important barriers: Firstly, the offer must indeed be *untrue*. If the offer actually ends after such a short period of time, the claim is not untrue, even if the time window may have been set arbitrarily.[151] Furthermore, the period must be so short that the offer puts the consumer under such pressure that he or she can no longer make an informed decision. A one-week offer period, for example, is not generally considered to be such.[152]

No. 11 of Annex I prohibits *disguised ads* patterns in media. When editorial content is used in media for sales promotion purposes that the trader has paid for, the advertising nature of the content must be evident. The provision thus separates editorial and advertising content and is intended to prevent the special credibility of editorial content being used for product advertising.

The Omnibus Directive[153] introduced a ban on hidden advertising in search results with No. 11a of Annex I. This means that when search results are displayed, it is now mandatory to disclose if a product appears in the search results due to a payment or if the ranking of the product within the search results has been raised due to a payment. This addresses one of the cases from the study assigned by the EU Commission on *disguised ads* in the online retail sector[154] and also addresses *false hierarchy* patterns. Disclosure of the payment is sufficient if it is clearly recognisable to the average consumer. In the example, in the bottom right-hand corner of the ad, there is a grey notice „Ann.", which is a common abbreviation in Italy for „Annunci", i.e. advertising. Due to the chosen size of the notice, this could be a borderline case as to whether the labelling is recognisable to the average consumer.

No. 13 of Annex I prohibits a *bait and switch* pattern, namely the offer of a product that is similar to that of another supplier in order to mislead the consumer into believing that it is the original product.

---

151 See *Martini/Drews/Seeliger/Weinzierl*, ZfDR 2021, 47, 64.

152 *Köhler*, in: Köhler/Bornkamm/Feddersen (eds.), 2024, Annex to section 3 (3) para. 7.6.

153 Directive 2019/2161.

154 *Lupiáñez-Villanueva/Boluda/Bogliacino/Liva/Lechardoy/Rodríguez de las Heras Ballell*, Behavioural study on unfair commercial practices in the digital environment, 2022, Figure 5, P. 48, available at: https://op.europa.eu/en/publication-detail/-/publication/606365bc-d58b-11ec-a95f-01aa75ed71a1/language-en/format-PDF/source-257599418. See also B. V. 2. h) above.

No. 20 of Annex I prohibits the advertising of a product as "free of charge" if costs are nevertheless to be borne. This does not apply only if the costs are unavoidable, such as shipping costs or travelling expenses incurred by the consumer. Other costs, such as "handling fees", may not be charged by the trader.[155] This addresses in particular the practice of advertising goods or services as "free" and encouraging consumers to buy in order to then finance the goods via increased (not actually incurred) postage or handling charges. A frequent application of No. 20 of Annex I is therefore also subscription traps on the internet, where a longer-term contract is concluded when a supposedly free service is used.[156] Those *hidden costs* and *hidden subscription* patterns are therefore prohibited under the UCPD.

No. 21 and 29 of Annex I prohibit further "dark patterns" that can occur. The provisions prohibit practices of sending the consumer advertising material, unjustified requests for payment or even unsolicited goods in order to give the consumer the false impression that he or she must fulfil their obligation arising from a supposed contractual relationship.

A particular kind of *social proof* or *testimonial* pattern, which used to be very common on the internet, was added to Annex I of the UCPD with No. 23b and 23c as part of the Omnibus Directive. The new provisions prohibit the use of unverified or falsified product reviews by buyers.

The list in Annex I of the UCPD contains case-by-case bans that prohibit some dark patterns. However, they do not contain any systematic "dark patterns" controls, but rather address them randomly.[157] The list cannot be used for "dark patterns" that use similar mechanisms but do not fall under the offences in Annex I, as it is self-contained and not capable of analogy. However, it also does not restrict the other unfairness offences in the UCPD. Thus, situations that are not regulated by Annex I are not automatically authorised, but can be reviewed for unfairness in accordance with the general rules.[158]

b) Aggressive commercial practice, Art. 8 et seq. UCPD

Art. 8 UCPD prohibits aggressive commercial practices. This stipulates that the act must be commercially relevant. The consumer must therefore have acted differently as a result of the commer-

155 *Köhler*, in: Köhler/Bornkamm/Feddersen (eds.), 2024, Annex to Section 3 (3) para. 20.5.
156 *Alexander,* in: Heermann/Schlingloff (eds.), 2020, Section 3 (3) No. 21 para. 22.
157 See also *Martini/Drews/Seelinger/Weinzierl*, ZfDR 2021, 47, 65.
158 *Köhler*, in: Köhler/Bornkamm/Feddersen (eds.), 2024, Section 3 para. 4.4.

cial practice than he or she would have done without the practice. The act is aggressive if it significantly affects the individual case through harassment, coercion, including the use of physical force, or undue influence. In turn, undue influence exists if the trader exploits a market position vis-à-vis the consumer to exert pressure in such a way that the ability to make an informed decision is significantly impaired or at least objectively appears to be. Based on Art. 8 UCPD, Art. 9 UCPD standardises the circumstances to be taken into account when assessing the aggressiveness of the practice, such as the timing, formulations, the exploitation of specific unfortunate situations, the confrontation with burdensome or disproportionate obstacles of a non-contractual nature or threats of legally impermissible actions.

i. Addressing "dark patterns"

This addresses some of the effects of "dark patterns", as these are often based on pressure or harassment, such as *nagging* or *click-fatigue* patterns. The *roach motel* pattern is explicitly mentioned as an example in Art. 9 lit. d UCPD. It refers to the onerous or disproportionate difficulty of cancelling contracts, as can occasionally be the case with the cancellation of premium subscriptions.[159] However, other impairments such as the rationality of decisions can also be prohibited by Art. 8 et seq UCPD. A detriment can even be assumed if the consumer was not clearly and appropriately informed, as in the case of *hidden information* patterns.[160]

ii. Significance of the influence

However, the offence under Art. 8 UCPD presupposes that the influence on freedom of choice is "significant". This is intended to exclude everyday and socially acceptable cases from the offence, as it is part of the nature of competition to persuade customers to make a business decision and also to influence them. Art. 8 UCPD is therefore not intended to protect against "unreasonable" consumer decisions, but only to ensure autonomous decision-making in the market.[161] A clear line has not yet been developed for the threshold of significant influence because it must always "take into account all features and circumstances".[162] Some focus on the consequences of the business decision and thus want to see a de minimis clause in the "significance".[163] According to this, it would

159 See also *Martini/Drews/Seeliger/Weinzierl*, ZfDR 2021, 47, 66.
160 *Köhler*, in: Köhler/Bornkamm/Feddersen (eds.), 2024, Section 4a para. 1.33a with further references.
161 *Picht*, in: Harte-Bavendamm/Henning-Bodewig (eds.), 2021, Section 4a para. 124.
162 Art. 8 UCPD.
163 *Sosnitza*, in: Ohly/Sosnitza (eds.), Commentary on the German Unfair Competition Act (UWG), 2023, Section 4a para. 198; see also *Martini/Drews/Seeliger/Weinzierl*, ZfDR 2021, 47, 66.

depend on whether the consequences of contracts concluded through aggressive influence are significant for the consumer. However, the following argues against this: Art. 8 UCPD only places significance in the context of influencing freedom of choice, but not in the context of the obligations arising from the behaviour. This also follows from the modalities of the influence, all of which are not based on the consequences of the consumer's behaviour, but on the way in which the consumer is influenced. It is therefore correct to assume that the determination of significance must depend on how effectively practices influence the consumer's decision. *Glöckner's* view should therefore be followed, who considers an influence to be insignificant as long as the consumer recognises it and at least supports its content.[164] Subliminal and efficient mechanisms can therefore exceed the significance threshold, regardless of how unfavourable the consequences are for the consumer. This means that "dark patterns" with a subliminal effect, which result in the consumer's decision not corresponding to their actual wishes – which may, of course, be influenced – can be prohibited.

iii. Existence of an alternative action from Art. 8 UCPD

However, this would also require that the "dark pattern" acts as an unauthorised means of influence, i.e. is used by harassment, coercion, including the use of physical force, or undue influence. An act is generally considered to be harassing if it constitutes an intrusion into the consumer's privacy.[165] This refers in particular to unsolicited home visits, unsolicited communication or the unsolicited sending of goods.[166] In addition, it is also sufficient if a consumer or market participant is influenced in a socially inappropriate manner.[167] Repeated, frequent contact with the consumer, as characterised by *nagging* patterns*,* can therefore be qualified as a nuisance if it reaches such an intensity that the consumer's autonomy is impaired. [168]

A coercion is present if the addressee is pressurised into making a decision through the use of force or the threat of a serious disadvantage.[169] In contrast, the third means of influence, undue influence, is likely to be more relevant for "dark patterns". For example, promotional competitions can constitute undue influence if the purchasing behaviour of the addressee is no longer primarily based

164 *Glöckner*, in: Harte-Bavendamm/Henning-Bodewig (eds.), 2021, Introduction, paras. 487 et seq.
165 *Köhler*, in: Köhler/Bornkamm/Feddersen. (Eds.), 2024, Section 4a para. 1.40
166 *Köhler*, in: Köhler/Bornkamm/Feddersen (eds.), 2024, UWG § 4a paras. 1.42 et seq.
167 *Raue*, in: Heermann/Schlingloff (eds.), 2020, Section 4a para. 114.
168 *Scherer*, in: Fezer/Büscher/Obergfell (eds.), Commentary on the German Unfair Competition Act (UWG), 2016, Commentary, Section 4a para. 124.
169 *Raue*, in: Heermann/Schlingloff (eds.), 2020, Section 4a para. 130.

on factual considerations but on the chance of winning.[170] It seems conceivable that companies with a corresponding position of power could use "dark patterns" to create similar stimuli that push the consumer's rationality into the background, such as particularly aggressive *confirmshaming* patterns that are designed to lead to a particularly guilty conscience when rejecting a loyalty programme. However, there is no apparent case law on this. In the case of *toying with emotion* patterns such as *confirmshaming*, it must also be considered that these must reach a very significant level in order to trigger a prohibition request. The emotional influence of consumers is omnipresent in business life, and the mere arousal of emotions in an otherwise – in the online world – quite anonymous legal transaction between companies and consumers cannot *per se* exert such a high level of pressure on the consumer that unfair influence can be assumed in each and every case. For instance, the example of *confirmshaming* cited in the study assigned by the EU Commission,[171] in which the "No, I don't like savings" button is shown, is unlikely to reach such a level.

iv. Interim results

Art. 8 et seq. UCPD can be used to effectively combat such "dark patterns" that are based on harassment, coercion or other undue influence, in particular the exertion of pressure through positions of power, if these significantly influence the consumer. With a correct interpretation of the provision, significant influence is present if the type of influence is capable of efficiently influencing the consumer's decision, in particular because the addressee is not aware of the influence or does not at least support it. However, it should be noted that the "dark pattern" must also constitute an unauthorised means of influencing. Particularly harassing *nagging* patterns that push rationality into the background due to their persistence are conceivable. In addition, cases are imaginable in which the trader uses its power over the consumer to exert pressure on them to make an irrational decision, such as with particularly aggressive *confirmshaming*. In cases where influencing by means of one of the behavioural alternatives in Art. 8 UCPD is particularly effective or subliminal, "dark patterns" are therefore already prohibited *de lege lata*.

---

170 *German Federal Court of Justice (BGH)*, judgement of. 22/1/2009 – I ZR 31/06, para. 12 – *Jeder 100. Einkauf gratis.*

171 *Lupiáñez-Villanueva/Boluda/Bogliacino/Liva/Lechardoy/Rodríguez de las Heras Ballell*, Behavioural study on unfair commercial practices in the digital environment, 2022, figure 120, p. 288. available at: https://op.europa.eu/en/publication-detail/-/publication/606365bc-d58b-11ec-a95f-01aa75ed71a1/language-en/format-PDF/source-257599418.

c) Misleading actions, Art. 6 et seq. UCPD

Art. 6 et seq. UCPD prohibits misleading commercial behaviour. A practice is misleading if it contains information that is untrue or likely to deceive the average consumer. This makes it clear that not only objectively false information, but also information that creates a false impression in the mind of the addressee can be unfair.[172] This means that practices that manipulate or complicate the processing of information by the consumer may also be prohibited under this provision, even beyond the provision of simply untrue information. Therefore, apparent information on the scarce availability of goods, for example in the form of a *countdown* or *scarcity* pattern, may be covered by Art. 6 UCPD. Unlike in the case of No. 7 of Annex I of the UCPD,[173] the provision is applicable even if it is not per se an untrue statement in the absence of a subsequent announcement, for example at the end of the *countdown*, provided that the average consumer would assume a certain consequence due to the design. For this reason, *activity messages* can also fall under this category, since – as with *scarcity* patterns – they can urge the consumer to make a hasty decision by wrongly assuming that the product is in high demand and could soon be sold out. However, there is no apparent case law on this. Since even skilful negations can influence consumer expectations to such an extent that the consumer states the opposite of what he or she actually wants to state, *trick questions* can also fall under Art. 6 et seq. UCPD.[174] Furthermore, Art. 6 (1) lit. d UCPD can protect against individual price calculations[175] based on tracking mechanisms.[176] However, as this is a provision that ensures transparency, these practices are not prohibited, but merely have to be shown transparently. Traders are therefore not prevented from offering price advantages through personalisation, for example based on past purchasing behaviour, if they present the information, in particular the price, how the price was calculated, or the existence of a specific price advantage, transparently.

---

172 *German Federal Court of Justice (BGH)*, judgement of. 24/9/2013 – I ZR 89/12, para. 15 – *Matratzen Factory Outlet*.

173 See a) above.

174 See *Martini/Drews/Seeliger/Weinzierl*, ZfDR 2021, 47, 67.

175 However, according to a study conducted by *ibi research an der Universität Regensburg GmbH* and *trinnovative GmbH* on behalf of the German Federal Ministry of Justice and Consumer Protection, personalised prices are not yet occuring in e-commerce. The study is available at: https://www.bmj.de/SharedDocs/Publikationen/DE/Fachpublikationen/2021_Empirie_Studie.pdf?__blob=publicationFile&v=2.

176 Thus *Martini/Drews/Seeliger/Weinzierl*, ZfDR 2021, 47, 66, 67.

Art. 7 UCPD prohibits misleading information by omission. Art. 7 (2) UCPD contains a special transparency rule that prohibits the provision of material information in an unclear, incomprehensible, or ambiguous manner. The standard is thus intended to counter those "dark patterns" that contain correct information but hide it due to their wording or graphic design, as characterised by *hidden information* and *misdirection* patterns. Article 7 (4) of the UCPD contains an obligation for companies to provide certain information that is essential to the contract, some of which corresponds to the information obligations in Consumer Contract Law. Of particular relevance here is the mention of the total price[177], as well as – newly added – the terms of payment, delivery and performance,[178] so that *hidden information* patterns intended to disguise this information are covered.[179] A new provision for search fields on websites that are not search engines and on which products are offered by different traders or consumers was added as part of the Omnibus Directive in Art. 7 (4a) UCPD. Here – similar to the provision in Annex I to the UCPD[180] – the consumer must be informed of which parameters lead to the specific ranking of the products, as well as the relative weighting of these parameters. This counteracts *false hierarchy* patterns that are intended to pre-sort certain results for the consumer to influence them. Finally, Art. 7 (6) UCPD addresses the obligation – also introduced as part of the Omnibus Directive – for traders that make consumer reviews available to provide information on whether the reviewing consumers have actually purchased the product. This addresses a particular *social proof* patterns and extends the regulations on customer reviews in No. 23b and 23c of Annex I of the UCPD[181].

d) Advertising

Advertising as a commercial practice is an important application of the UCPD. In Germany alone, there is extensive case law on special offers, *bait-and-switch* offers and price gouging, which can be misleading according to Art. 6 UCPD.[182] For example, it is misleading if a company advertises price reductions that are not actually offered because the product was never offered at the claimed,

177 Art. 7 (4) lit. c UCPD.
178 Art. 7 (4) lit. d UCPD.
179 See *Martini/Drews/Seeliger/Weinzierl*, ZfDR 2021, 47, 67; for example, failure to mention additional costs for baggage when booking a flight falls under this, see Higher Regional Court of Dresden, decision of 11/2/2020 – 14 U 1885/19.
180 On No. 11a of Annex I of the UCPD, see a) above.
181 See a) above.
182 See the comprehensive descriptions in *Sosnitza* in: Ohly/Sosnitza (eds.), 2023, Section 5 para. 239 et seq.

unreduced original price.[183] By now, Art. 6a of the Price Indication Directive[184] was implemented and contains detailed regulations for information on price reductions, so that special provisions now exist.

e) General clause, Art. 5 (2) UCPD

As a catch-all provision, Art. 5 (2) UCPD contains a general clause that can deal with unfair cases that are not covered by the more specific provisions. This includes, for example, "dark patterns" that are not effective enough to influence or that do not use the appropriate means of influence to fall under Art. 8 UCPD, but the consequences for the addressee are undesirable to such extent that there is a need to prohibit the practice.

According to Art. 5 (2) UCPD, commercial activities that are directed at or reach consumers are unfair if they do not comply with professional diligence and are likely to materially influence the consumer's economic behaviour. Unlike the other provisions in the UCPD, the prerequisite of "materiality" is included, which excludes minor cases from the scope of the provision.[185] "Professional diligence" means the standard of special skill and care when a trader may reasonable be expected to exercise towards consumers, commensurate with honest market practice and/or the general principle of good faith in the trader's field of activity.[186]

It requires an overall assessment of the circumstances, whereby the intensity of the commercial behaviour, the market strength of the company, the degree of culpability and the nature of the legal interests affected are among the decisive factors.[187] In Germany commercial behaviour was assumed material in this context and thus Art. 5 (2) UCPD applied due to a particular incentive or luring effect with certain practices.[188] It can therefore be assumed that effective "dark patterns", irrelevant of their category, can fall under the scope of Art. 5 (2) UCPD.[189]

---

183 See *German Federal Court of Justice (BGH)*, judgement of 8/12/1978 – I ZR 57/77 – *10-Jahres-Jubiläum*.

184 Directive 98/6/EC, whose application has led to problems and is subject to discussion, see for instance: https://www.eurocommerce.eu/app/uploads/2024/03/20240229-pid-joint-paper-ee-eurocommerce-ire-final.pdf.

185 *Sosnitza*, in: Heermann/Schlingloff (eds.), 2020, Section 3 para. 126.

186 Art. 2 lit. h UCPD.

187 See *Sosnitza*, in: Heermann/Schlingloff (eds.), 2020, Section 3 para. 128 et seq.

188 See the references in *Sosnitza*, in: Heermann/Schlingloff (eds.), 2020, Section 3 para. 135, footnote 357.

189 See also *Martini/Drews/Seeliger/Weinzierl*, ZfDR 2021, 47, 68.

f) Interim result

Although the UCPD does not systematically deal with "dark patterns",its provisions seem suitable for effectively countering them. The legislator's approach is very similar to that of Consumer Contract Law. For the most part, "dark patterns" are subject to fine-grained prohibitions, such as in Annex I of the UCPD or Art. 5 et seq. UCPD explicitly. If the legislator identifies a practice that has not yet been addressed and in which a manipulative design triggers a need for a ban, it can make adjustments by creating special provisions, as it recently did via the Omnibus Directive. Otherwise, it will be possible to regulate "dark patterns", at least if they are particularly effective, via Art. 5 (2) UCPD and, if necessary, prohibit them. This means that case law can effectively close regulatory gaps in individual cases if the facts of the case justify the need for a broader legislative intervention in terms of the effectiveness of the influence and the severity of the consequences. There is therefore currently no apparent need for a comprehensive ban on "dark patterns" in the UCPD.

Enforcement deficits that exist in Consumer Contract Law as the consumer is primarily responsible for the enforcement are also effectively eliminated by the UCPD. The prohibitions can be enforced not only by those affected,[190] but also by other persons and associations such as competitors or consumer organisations in accordance with the law of the Member State.[191] This means that market guardians are empowered to take action against infringements, which may not seem attractive to individual consumers due to the hurdles and effort involved in litigation.

3. Applicability of Consumer Law with traders outside of the EU

A further issue in the question of the enforcement of consumer law arises when the trader is not based in the EU. In order to achieve a high level of consumer protection in an international context, there are numerous regulations that ensure the applicability of Consumer Law. As this is closely linked to the effectiveness of consumer protection, it is necessary to briefly discuss which provisions also cover the issues raised here internationally.

190 Inserted by the Omnibus Directive in Art. 11a UCPD.
191 Art. 11 UCPD.

a) Art. 6 Rome I Regulation

Art. 6 Rome I Regulation[192] is a special conflict-of-law rule for consumer contracts. This clarifies that, in the case of consumer contracts, the regulatory regime in which the consumer has his habitual residence generally applies. However, only the "passive consumer" who is exposed to the economic activities of foreign traders at home is protected. If the consumer goes abroad to interact with a trader based there, the provision does not apply.

In addition, according to Art. 6 (1) lit. a Rome I Regulation, the trader must carry out his professional or commercial activities in the country of habitual residence. According to Art. 6 (1) lit. b Rome I Regulation, it is even sufficient for the trader to direct the activity to the country of habitual residence. For example, it is sufficient for the trader to advertise his offer in Germany, for the consumer to take note of the advertising and then make a purchase. This therefore includes cases in which foreign traders expressly offer their goods for dispatch to the EU country, as the trader thus expresses his willingness to conclude a contract with EU consumers.[193]

As the Rome I Regulation relates to contractual obligations, actions by consumers can at least be based on this provision. In the case of consumer association and competitor actions, it was disputed whether this provision applies,[194] although this now falls under Art. 6 Rome II Regulation.

b) Art. 6 Rome II Regulation

Art. 6 Rome II Regulation contains a collision rule for unfair commercial practices in an international context. Art. 6 para. 1 Rome II Regulation clarifies that the law of the state in whose territory the competitive relations or the collective interests of consumers have been or are likely to be affected is applicable. The ECJ has clarified that this also applies to actions for injunctions against general terms and conditions by consumer associations.[195] Therefore, the standards of the European Union also apply to injunctive relief under the UCPD if the trader is based outside the EU but its business activities have an impact on consumers in the EU.

192 Regulation 864/2007.

193 *Kreuzer/Wagner/Reder*, in: Dauses/Ludwigs (eds.), Handbook of EU Business Law, 2023, R. 2. f) bb) ccc) paras. 176 et. seq.

194 *Drexl*, in: Säcker/Rixecker/Oetker/Limperg (eds.), Art. 6 Rome II Regulation, paras. 135 et seq.

195 *ECJ*, judgement of 28/7/2016 – C-191/15.

c) Interim result

At first glance, the regulations ensure that consumers, consumer organisations and competitors can enforce their rights under the Consumer Contracts Law and the UCPD. The comprehensive regulatory regime can therefore not simply be cancelled out by traders operating from outside the EU.

4. Data Protection Law

Data Protection Law is a matter that is addressed particularly frequently with regard to "dark patterns". One reason for this is that the field of electronic data processing provides a particularly favourable environment for influencing interface designs.[196] In addition, a growing number of data-driven business models as a result of advancing digitalisation means that there is an increased need to process personal data. Depending on the applicable regulations, various justifications for data processing can be considered. These can, inter alia, be consent, the necessity for the fulfilment of a contract or the protection of legitimate interests.[197]

Although this development has been going on for some time, the requirements for consent have basically remained unchanged since the Data Protection Directive[198] more than 25 years ago. Consent must be given voluntarily and in an informed manner.[199] It must be emphasised that as soon as Data Protection Law is applicable, data processors are subject to special accountability obligations, which makes it easier to provide evidence, Art. 5 (2) GDPR. In addition, there are regulatory options for data protection-friendly technology design, Art. 25 GDPR.

The importance of Data Protection Law is also particularly virulent in the area of Consumer Law, as consumers are regularly affected by data processing in data-driven business models. In the context of "digital fairness", BEUC therefore associates in a large number of cases the processing of personal data with a feeling of "unfairness" on the part of the data subjects.[200] It must therefore be shown overall whether the provisions of the GDPR, the central data protection act, are sufficient to establish digital fairness.

---

196 See *Martini/Drews/Seeliger/Weinzierl*, ZfDR 2021, 47, 50.

197 Art. 6 (1) GDPR.

198 Directive 95/46/EC.

199 Art. 2(h) of the Data Protection Directive states that consent is "[…] any freely given specific and informed indication".

200 See *BEUC*, Connected but unfairly treated, available at: https://www.beuc.eu/sites/default/files/publications/BEUC-X-2023-113_Fairness_of_the_digital_environment_survey_results.pdf.

a) Consent, Art. 4 No. 11, Art. 7 GDPR

The instrument of consent is of particular relevance when addressing "dark patterns", as a large proportion of the case studies mentioned relate to the design of so-called "cookie banners" or „consent banners". These are interfaces in which the user is asked for their consent to store or read cookies on their end device. These cookies, as well as other similar technologies, are required to track the user and thus create a profile about them. Legally, this action generally requires consent, Art. 5 (3) ePrivacy Directive[201]. This is then based solely on the requirements of the GDPR.[202]
It should also be taken into account that consent as a justification for data processing is already particularly emphasised from a fundamental rights perspective.[203] It is voluntary and informed consent that is an expression of the digital sovereignty of the data subject. The requirements for the effectiveness of consent must therefore not degenerate into a mere fiction. On the other hand, digital sovereignty is not paternalistic in nature, but rather requires that any type of data processing can be legitimised by consent if it is based on transparency and voluntariness. Otherwise, the controlling power of digital sovereignty would be jeopardised.[204] It is therefore of paramount importance in data-driven business models.

i. Voluntary consent, Art. 4 No. 11 GDPR[205]

Art. 4 No. 11 GDPR defines consent as a voluntary expression of will. The requirement that consent must be voluntary in order to be effective reflects the legal reality that often, unequal partners face each other. The consent of the weaker partner is at risk of losing its legitimising effect for the encroachment on their right to informational self-determination if, due to factual circumstances, there is no free choice and the data subject must consent in order to receive or retain the desired service.[206] The same applies if the data subject is induced to disclose [their] data by "excessive incentives of a financial or other nature".[207] Overall, the criteria of imbalance, necessity, contractual performance, reasonable alternative and an appropriate balance of interests are therefore relevant for the assessment of voluntariness.

---

201 Directive 2002/58/EC. Whether this regulation is appropriate or whether other justifications, such as those of the GDPR, should be used in a possible ePrivacy Regulation is the subject of debate, see *Kühling*, CR 2020, 199, 202.
202 Art. 94 GDPR.
203 See 1.c) above.
204 *Buchner/Kühling*, in: Kühling/Buchner (eds.), Commentary on the GDPR and the German Data Protection Act, 2024, Art. 7 GDPR para. 41.
205 This section is based on *Kühling/Klar/Sackmann*, Data Protection Law, 2021, paras. 512 et seq.
206 See *German Federal Constitutional Court (BVerfG)*, decision of 25/31992, 1 BvR 1430/88.
207 *German Federal Court of Justice (BGH)*, judgement of 16/7/2008, VIII ZR 348/06, para. 21.

From the requirement of voluntariness, the body of the German Data Protection Supervisory Authorities DSK[208] wants to conclude, in conjunction with the principle of data minimisation, that the creation of a user profile in online shops is only voluntary if free guest access is also provided.[209] The DSK is thus directly addressing *forced registration* patterns.

However, the generalisation with which the DSK rejects voluntariness is difficult to reconcile with the requirements of the GDPR.[210] It should be emphasised that the requirements for voluntariness depend on a variety of factors, which are explained below. If an online retailer obliges the consumer to create an account to use their service, consent is not involuntary *per se*. For example, it is conceivable that in the case of online retailers that do not have market power, the customer could choose to order from another retailer, which is why the creation of a profile would be voluntary even without the option of a guest access. Nevertheless, the voluntary nature of consent can be used to create a system that prohibits *forced registration* patterns in special constellations.

ii. Imbalance between the players

Recital 43 of the GDPR states that consent can be involuntary if there is a clear imbalance between the parties involved. Typical examples of this are employment relationships and the relationship between citizen and the state, but in individual cases also relationships between traders and consumers.[211] The European Court of Human Rights[212] states that the right to the protection of personal data is not to be guaranteed without limits, but must be harmonised with the Convention rights of others. In this context, the Court also recognises the state's duty to protect in cases where only private individuals are involved.[213] Also, the German Federal Constitutional Court stated that if it is evident that one partner in a contractual relationship has such weight that it can in fact unilaterally determine the content of the contract, it is the task of the legislator to work towards safeguarding the fundamental rights of both contractual partners in order to prevent self-determination from

208 "Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder".

209 Available at: https://datenschutzkonferenz-online.de/media/dskb/20222604_beschluss_datenminimierung_onlinehandel.pdf.

210 The DSK's position has therefore been criticised, see, for example, *GDD*, Stellungnahme zum DSK-Beschluss „Datenschutzkonformer Online-Handel mittels Gastzugang" und zur Werbung, available at: https://www.gdd.de/aktuelles/gdd-stellungnahme-zum-dsk-beschluss/.

211 For example, in the case of monopolists, see *Buchner*, Datenschutz und Datensicherheit (DuD) 2016, 155, 158.

212 ECtHR.

213 *ECtHR*, Decision of 2/12/2008, No. 2872/02, para. 49 – *K.U./Finland*. See also *Kühling/Klar/Sackmann*, Data Protection Law, 2021, paras. 31, 41.

turning into heteronomy for one party.[214] It is true that this decision does not bind the GDPR as an EU regulation. However, these principles are also likely to apply at Union level.

iii. Prohibition of tying, Art. 7 (4) GDPR

The prohibition of tying under Art. 7 (4) GDPR is violated if the fulfilment or conclusion of a contract is made dependent on consent that is not required for the fulfilment of the contract. However, the data processor is not prohibited from making its performance dependent on the granting of consent in the sense of "take it or leave it". For this to be the case, however, all data processing to which consent is given must be necessary for the fulfilment of the contract.[215] In these cases, however, due to the necessity for the fulfilment of the contract, permissibility according to Art. 6 (1) (1) lit. b GDPR will regularly already exist. On the other hand, consent can make the provision of personal data itself the subject of the main performance obligation, for example in the case of exchange of data for services, as is the case with social networks.[216] To assess the necessity, the specific characteristics of the service provided by the controller must also be determined, which opens up a transparent model of data in exchange for services, especially for the "online world".[217] It also plays a role whether the data subject has a reasonable alternative available on the market for the desired conclusion of the contract,[218] which is not the case with large social networks, for example, on whose use one can be partially dependent for establishing contact with other persons. In addition, the criterion of an appropriate balance of interests must also be taken into account in the overall assessment.[219] The ECJ recently applied strict rules on consent of market dominant companies but nevertheless accepted the business model of data in exchange for services under the conditions of a fairness in the commercialisation of data. It ruled that consent might be voluntary with large social networks if a monetary payment is demanded in the event of refusal in the case of fine-grained consent options, as long as the payment is appropriate.[220]

This also addresses "dark patterns" that require consent to data processing for the provision of a completely unrelated service, such as image processing software that allows consent to location

214 *BVerfG*, decision of 23/10/2006, 1 BvR 2027/02.
215 *Buchner/Kühling*, in: Kühling/Buchner (eds.), Art. 7 GDPR paras. 41 et seq.
216 *Buchner/Kühling*, in: Kühling/Buchner (eds.), 2024, Art. 7 GDPR para. 51 et seq.
217 *Buchner/Kühling*, in: Kühling/Buchner (eds.), 2024, Art. 7 GDPR para. 49.
218 *Buchner/Kühling*, in: Kühling/Buchner (eds.), 2024, Art. 7 GDPR para. 52 et seq.
219 *Buchner/Kühling*, in: Kühling/Buchner (eds.), 2024, Art. 7 GDPR para. 54.
220 *ECJ,* Decision of 4/7/2023 – C-252/21, paras. 149 et seq. See also *Buchner/Kühling*, in: Kühling/Buchner (eds.), 2024, Art. 7 GDPR para. 53c.

tracking or storage.[221] Repeated requests for consent or making it unnecessarily difficult to refuse consent can also cast doubt on the voluntary nature of consent.[222] The benchmark here must be whether the design of the consent options primarily serves the purpose of pressurising the user to give consent or whether it is necessary in order to make detailed settings.

iv. Comparison with rules governing general terms and conditions

The regulations on consent under Data Protection Law are very similar with respect to the control of general terms and conditions under Consumer Contract Law. In both cases, private autonomy is the starting point. This is jeopardised in the case of unequal contractual partners, as the weaker party is ultimately no longer free to decide. In addition, they often no longer have time to realise the implications of its declaration. There are therefore arguments in favour of using the idea of checking for the existence of an "significant imbalance of the parties' rights and obligations […] to the detriment of the consumer", Art. 3 (1) of the UCTD, which originates from the provision on general terms and conditions, as a key criterion. Consent that is strongly to the detriment of the person concerned and against their objective interests indicates doubts as to its voluntary nature.[223] As a result, it is only possible to speak of a free decision by data subjects if they effectively have the opportunity to determine whether and how their data is processed. If data subject's consent is not based on their free decision, their consent is invalid and data that has already been collected must be deleted.

Like Consumer Contract Law, the UCPD and the UCTD are characterised by general clauses that are supplemented by individual case regulations. In terms of the system of provisions, this is the main difference to Data Protection Law, which does not regulate specific individual cases in the case of consent, but instead consists exclusively of general clauses.

v. Informed consent, Art. 4 No. 11 GDPR[224]

In addition, Art. 4 No. 11 GDPR stipulates that consent must be given in an informed manner. Only a data subject who is aware of all information relevant to the decision can assess the risks and benefits of consent and make a decision based on this. Their consent can therefore only relate to

221 See *Martini/Drews/Seelinger/Weinzierl,* ZfDR 2021, 47, 55 with reference to *European Data Protection Board*, Guidelines 5/2020 on consent under Regulation 2016/679, 4 May 2020, p. 19.

222 See *Martini/Drews/Seelinger/Weinzierl,* ZfDR 2021, 47, 55.

223 *Buchner/Kühling*, in: Kühling/Buchner (eds.), 2024, Art. 7 GDPR, para. 54.

224 This section is based on *Kühling/Klar/Sackmann*, Data Protection Law, 2021, para. 517 et seq.

known circumstances. It is therefore not possible to effectively consent to unknown data processing. The controller therefore has a comprehensive duty to provide information, in particular with regard to the types of data processed, the purpose of processing, the identity of the controller and its availability and, if applicable, the data recipients. The obligation to provide information must take place before consent is obtained, whereby the details follow from Art. 12 and 13 GDPR. It is not sufficient, for example, if the impression is initially given that the information is about scientific or other findings, but it is about the use of data for subsequent sales purposes.[225]
The requirement to be informed prevents practices that rely on the concealment of information, such as *hidden information* patterns.

vi. Specific consent

Closely related to the duty to inform is the requirement for the declaration of consent to be specific, which is derived directly from the principle of purpose limitation as stipulated in Art. 5 (1) lit. c GDPR.[226] The data subject can only assess the benefits and risks of their consent if they understand the content of the consent and the declaration of consent is sufficiently specific.[227]
In order to fulfil the requirement of specifically declaring, not only the data or the type of data must be named, but in principle also the individual concrete phases of data processing. However, the required degree of certainty can only be determined in conjunction with the specific processing situation. The more complex the processing phases and the higher their number, the less the naming of each individual processing step can be required. In these cases, it is sufficient to describe the essential phases of processing. For reasons of comprehensibility and clarity, a certain degree of incompleteness must be accepted. Conversely, the more the protection of the data subject's privacy is affected, the higher the requirements for certainty.
Consent can only ever relate to specific data processing for precisely defined purposes. Blanket consent is therefore invalid. [228]

225 For instance, *Regional Court of Traunstein*, judgement of 20/5/2008, 7 O 318/08.
226 *Buchner/Kühling*, in: Kühling/Buchner (eds.), 2024, Art. 7 GDPR para. 61 with further references.
227 One possible exception, which is discussed under the keyword "broad consent", is in the area of scientific research, see Recital 33 GDPR.
228 On the old version of the German Data Protection Act (BDSG), for example *BGH*, judgement of. 19/09/1985, III ZR 213/83; *BGH*, judgement of 10/7/1991, VIII ZR 296/90; *BGH*, judgement v. 11/12/1991, VIII ZR 4/91.

vii. Transparency requirement, Art. 7 (2), Art. 5 (1) lit. a GDPR

In order to prevent declarations of consent from being *hidden*, Art. 7 (2) 1 GDPR requires the consent to be emphasised as a special form of the transparency requirement of Art. 5 (1) lit. a GDPR.[229] The consent text must stand out visually from the other declarations and be appropriately positioned. If this is not the case, consent is invalid and data processing is unlawful. Furthermore, the text which is pre-formulated by the controller must clearly and comprehensibly explain to the data subject the content of the consent, and must not be given together with other declarations. .[230]

viii. Consent by declaration or clearly confirming action, Art. 4 No. 11 GDPR

The GDPR also stipulates that consent must be given explicitly. This means that consent given through pre-selected settings or pre-ticked checkboxes, the so-called opt-out, is invalid, Art. 4 No. 11 and Recital 32 GDPR.[231] In addition, the data subject must be aware that he or she is declaring something legally relevant when giving consent (awareness of consent). This also prohibits practices like *preselection* that seek to provoke a declaration of consent through tricky interface designs that resemble an opt-out, such as a labelled button and a pre-filled checkbox.[232] Implied declarations of consent, for example by simply scrolling on a homepage, are no longer possible at all.[233] Finally, *trick questions* that make the consumer choose the opposite of the statement they actually wanted to explain clearly do not fulfil the requirements of a confirming action.[234]

ix. Revocation, Art. 7 (3) GDPR

Similar to Consumer Contract Law, Data Protection Law also recognises the possibility of unconditional withdrawal in Art. 7 (3) GDPR.[235] However, this differs from its counterpart under Consumer Contract Law in several respects. Firstly, it is not tied to a time limit, but can be exercised "at any time", Art. 7 (3) 1 GDPR. Secondly, it does not completely remove the consequences of the processing and lead to a reversal, but removes the effectiveness of the consent from the moment of the declaration. Revocation under Data Protection Law thus ultimately represents an expression

229 *Tinnefeld/Buchner et al.*., Introduction to Data Protection Law, 7th ed. 2019, p. 418.
230 See also *Ernst*, ZD 2017, 110, 113.
231 Recently *ECJ*, judgement of 1/10/2019 – C-673/17, paras. 55-65 - *Planet49*; see also *Kühling/Sauerborn*, CR 2021, 271, 279.
232 *Buchner/Kühling*, in: Kühling/Buchner (eds.), 2024, Art. 7 GDPR para. 58a with further references.
233 See *Buchner/Kühling*, in: Kühling/Buchner (eds.), 2024, Art. 7 GDPR paras. 58b, 58c.
234 See *Martini/Drews/Seeliger/Weinzierl*, ZfDR 2021, 47, 55 f.
235 See 1. e) above.

of the voluntary nature of the declaration of consent,[236] while cancellation under Consumer Contract Law is intended to cancel a commitment that was entered into due to a surprise or informational deficits. To ensure that the right to revocation is not artificially complicated, it must be as simple as expressing consent, Art. 7 (3) 4 GDPR. In addition, the data subject must be informed of their right of withdrawal before expressing consent, Art. 7 (3) 3 GDPR. This prevents *roach motel* patterns in data processing situations requiring consent.

x. Interim result

Consent is in principle an effective instrument for ensuring the digital sovereignty of data subjects. It is a carefully balanced tool that ensures that consent corresponds to the actual will of the data subject. The mechanisms of consent ensure that the consent corresponds to the actual will of the data subject.

It therefore seems surprising at first glance that the BEUC study[237] shows, for example, that 60% of consumers surveyed find personal data analysis and monetisation unfair. This might be the case as in a lot of cases the mechanisms of consent are not working in practice, i.e. the voluntariness or transparency are not guaranteed. But this is not a question of having enough legal safeguards but a question of enforcing the current law effectively. The decision of the ECJ in the Facebook case[238] can be interpreted as a first step to guarantee fairness in the monetisation of personal data.

However, it should be noted that the monetisation of personal data in data-driven business models is what ensures the financing of services in the first place. These are concepts of "data in exchange for services", in which the data subject is generally exempt from paying a fee or this is at least partially replaced by monetisation of the data. If the conditions for consent are met, i.e. in particular if there are alternatives on the market that do not require consent, which is why consent was given voluntarily, the data processing should not be considered unfair *per se*. Again, it is therefore more likely that there is either a lack of enforcement of the data protection regulations, so that the consent does not actually correspond to the will of the data subjects. In any case the services asked for by the customers must be financed – either by payments or by consuming advertising (which is all the more valuable for the provider if it is based on data of the costumers) or by a mixture of payments

236 See *Kühling/Klar/Sackmann*, Data Protection Law, 2021, para. 529.

237 *BEUC*, Connected but unfairly treated, p. 4 et seq., available at: https://www.beuc.eu/sites/default/files/publications/BEUC-X-2023-113_Fairness_of_the_digital_environment_survey_results.pdf.

238 *ECJ,* Decision of 4/7/2023 – C-252/21, paras. 149 et seq. See also *Buchner/Kühling*, in: Kühling/Buchner (eds.), 2024, Art. 7 GDPR para. 53a et seq.

and advertisements. This is basically the idea of the so-called "pay or okay" or "PURl"-modell,[239] which is now explicitly considered permissible by some data protection authorities[240] and which the ECJ[241] has recently legitimised in general. The voluntary nature of consent is ensured by offering the service alternatively for a fee, but without data monetarisation. Insofar as the fee charged is reasonable or "fair", there are no fundamental objections to this. Data subjects who find the monetisation of their data unfair thus have the option of using the same provider's service for a fee without their data being used to finance it.

b) Accountability under Data Protection Law, Art. 5 (2) GDPR

Art. 5 (2) GDPR contains the accountability obligation for the controller. On the one hand, this includes the assignment of responsibility for compliance with the data protection principles of Art. 5 (1) GDPR. Despite the reference to just one paragraph, this means a very high extent of responsibility, as the principles of Data Protection Law in Art. 5 (1) GDPR are very far-reaching. As a rule, the controller is effectively responsible for its entire data processing.

From Art. 5 (2) GDPR, it can also be concluded that the controller must prove the lawfulness of the data processing. In fact, this results in a reversal of the burden of proof in the area of Data Protection Law.[242]

c) Privacy by design and by default, Art. 25 GDPR

The requirements of Art. 25 GDPR on "privacy by design" and "privacy by default" are closely linked to the provisions on consent, but are at a more general level of requirements.[243] The former describes the obligation to design products in such a way that they already take data protection concerns into account during their development, taking into account the associated costs and other

---

239 See *Kühling/Sauerborn*, Rechtsgutachten über die "Herausforderungen für Telemedienanbieter bei der Compliance mit den Vorgaben des TTDSG und der DS-GVO", p. 21 et seq., available at: https://www.datenschutzkonferenz-online.de/media/ko/13b_Kuehling-Sauerborn-Gutachten-ZAW-25-26-TTDSG-final.pdf.

240 *DSK*, Bewertung von Pur-Abo-Modellen auf Websites, available at: https://www.bfdi.bund.de/SharedDocs/Downloads/DE/DSK/DSKBeschluessePositionspapiere/DSK_20230322-Pur-Abo-Modelle.pdf?__blob=publicationFile&v=1 .s. *Austrian Data Protection Authority*, Decision of 30/11/2018, available at: https://www.ris.bka.gv.at/Dokumente/Dsk/DSBT_20181130_DSB_D122_931_0003_DSB_2018_00/DSBT_20181130_DSB_D122_931_0003_DSB_2018_00.pdf.

241 *ECJ,* Decision of 4/7/2023 – C-252/21, paras. 149 et seq. See also *Buchner/Kühling*, in: Kühling/Buchner (eds.), 2024, Art. 7 GDPR para. 53a et seq.

242 See *Herbst*, in: Kühling/Buchner (eds.), 2024, Art. 5 GDPR paras. 79 et seq. On the reversal of the burden of proof in civil procedure see for instance *Higher Regional Court of Stuttgart*, 18/5/2021 – 12 U 296/20.

243 The following section is based on *Kühling/Klar/Sackmann*, Data Protection Law, 2021, paras. 757 et seq.

disadvantages. This obligation does not only apply to physical products, but also to online services.[244] In practice, proof of data protection-compliant product design can be provided through approved certification procedures in accordance with Art. 25 (3) GDPR. Violation of the obligation to design products in a data protection-friendly manner is subject to fines, Art. 83 (4) lit. a GDPR. "Privacy by default" describes the obligation of the controller to design configurable working methods of its products in such a way that, by default, only personal data that is necessary for the specific processing purpose is processed. If the data subject wishes to use additional functions that involve further data processing, they must actively change the settings. Systematically, this provision is therefore to be found in the enforcement of the voluntary nature of consent and the opt-in principle.[245] In this respect, the explanations on consent above can be taken up.

Overall, the accompanying requirements of avoiding undue influence through data protection by design have a supplementary significance for the prevention of undesirable "dark patterns". However, this also requires specification in individual cases. In view of the very rough nature of the requirements and the lack of fine-grained determination of the limit of a still acceptable influence, particularly strong *nagging* patterns and problematic one-sided and strongly guiding *default* patterns are filtered out. It is questionable if this also applies to merely weak *misdirection* patterns.[246]

d) Applicability of the GDPR for processors located outside the EU

According to Art. 3 (2) GDPR, the "marketplace principle" governs the applicability of the provisions of the GDPR by processors based outside the EU member states. This was preceded by a much-noticed decision by the ECJ[247] on the Data Protection Directive, which was then incorporated into the GDPR.

According to Art. 3 para. 2 GDPR, the GDPR applies if the data processing is carried out by a controller or processor in another EU country and is related to the offering of goods or services to the data subject, or the monitoring of the data subject's behaviour, insofar as the behaviour takes place in the European Union. Enforcement of Data Protection Law is facilitated by the obligation

244 *Hamann*, Betriebsberater (BB) 2017, 1090, 1095.

245 To a large extent *Wolff*, in: Schantz/Wolff (eds.), The new Data Protection Law, 2017, para. 840, who recognises a major innovation of the GDPR in this provision.

246 See also *Martini/Drews/Seeliger/Weinzierl*, ZfDR 2021, 47, 57, with the examples of inadmissible persistent requests for consent on the one hand and the still permissible, influence-driven colour design of buttons in green and red on the other, as well as with reference to *European Data Protection Board*, Guidelines 5/2020 on consent under Regulation 2016/679, 4/5/2020, p. 19.

247 *ECJ*, decision of 13/5/2014 – C-131/12, para. 55.

to appoint a representative in the EU for data processors outside the EU, which is subject to fines.[248] In the case of the sectors of online trading and online B2C marketplaces analysed here, as well as the tracking of data subjects, the GDPR therefore applies without restriction in accordance with the marketplace principle. Here again it is of course important to have an effective enforcement of the existing rules.

e) Interim results

This results in a similar interim conclusion as with regard to the analysis under Consumer Contract and the UCPD: numerous particularly problematic cases of "dark patterns" are already covered by the sufficiently strict applicable law, particularly in the GDPR, insofar as they are based on data processing. The strict sanctions regime of the GDPR[249] should also have a deterrent effect on unauthorised "dark patterns" as soon as the first effective sanctions are imposed. Further additions may be expected here from the currently unclear development of the ePrivacy Regulation.[250] However, there is a major difference to Consumer Contract Law and the UCPD in that Data Protection Law relies more heavily on general provisions that are not supplemented by specific special offences. This makes it necessary to ensure sufficient standards of protection when applying the existing regulations. However, this is certainly possible if, for example, when determining the voluntariness of consent under parameters to be defined in more detail – and especially in the case of market-dominant providers – a commercialisation fairness is required and thus the excessive tapping of data is prevented.[251] The recent judgement of the ECJ in the *Facebook* case shows that this is feasible.[252]

In view of the additional control of unlawful interference through data protection by design and default in accordance with Art. 25 GDPR, there are therefore in principle sufficient tools for an appropriate normative response to data-based "dark patterns". This is particularly true as the applicable Secondary Union Law provisions are always interpreted by the ECJ in strict conformity with fundamental Data Protection Law[253], which has by no means led to an inadequate data protection standard to date.[254] Adjustments *de lege ferenda* would have to be made at Union level, as they

248 Art. 27, 83 (4) GDPR, see *Klar*, in: Kühling/Buchner (eds.), Art. 3 para. 27.
249 For an overview, see *Kühling/Klar/Sackmann*, Data Protection Law, 2021, paras. 790 et seq.
250 See the note by *Martini/Drews/Seeliger/Weinzierl*, ZfDR 2021, 47, 54 et seq.
251 *Martini/Drews/Seeliger/Weinzierl*, ZfDR 2021, 47, 59 are more sceptical in this respect.
252 See a) iii. above.
253 See I. 1. c) above.
254 *Kühling/Raab*, in: Kühling/Buchner (eds.), 2024, Introduction para. 31, provide a fundamental explanation and point out the risk of overly strong suppression of opposing protection concerns.

ultimately essentially represent a concretisation of the Union Law provisions on consent (and Art. 25 GDPR). However, this would contradict the general regulatory approach of EU Data Protection Law, which does not standardise fine-grained, sector-specific solutions to problems and works well with this approach. The consent regime has been essentially stable in terms of substantive law since 1995 and is able to cope with the issues of "dark patterns", If this is not the case, it is likely that the remaining "dark patterns" are not so powerful that sector-specific provisions at Union level are required for this very purpose and general law is not sufficient.

5. Other provisions

There are also provisions in other areas that can address "dark patterns".

a) Special provisions for "inbox advertising", Art. 13 (1) ePrivacy Directive

Until now, the question of how so-called "inbox advertising" should be assessed was unresolved. This is a particular *misdirection* or *bait-and-switch* pattern that displays advertisements in the inbox of a webmail service that are labelled „ad", „advertisement" or similar, which are often highlighted in a different colour. The German Federal Court of Justice referred the question to the ECJ as to whether "inbox advertising" constitutes email advertising requiring consent in accordance with Art. 13 (1) ePrivacy Directive. According to this provision, email advertising is only permitted if the addressee has given their prior consent. In this respect, the ECJ ruled that the legal categorisation of advertising as electronic communication is not relevant in the case of "inbox advertising",[255] but due to the appearance of the advertising, which resembles spam messages, and the risk of confusion with actual emails,[256] decided that "inbox advertising" must be treated in accordance with the provisions on email advertising. Therefore, a mere labelling as advertising is not sufficient. Instead, explicit consent in the advertising according to the provisions of the GDPR is required.

In this case, the ECJ therefore subjects this practice to a stricter regime due to the appearance of advertising, which must be measured against the imitated object. This type of case law can be used to counter those "dark patterns" which, due to habituation to certain behaviours (in this case, opening an email in the mailbox), result in other actions than those desired, and which also impose special requirements on these actions.

255 *ECJ*, judgement of 25/11/2021, C-102/20, para. 46 – *eprimo*.
256 *ECJ*, judgement of 25/11/2021, C-102/20, paras. 42 et seq – *eprimo*.

b) The Digital Services Act

For the first time, "dark patterns" have been explicitly discussed at EU level in the DSA legislative process. For example, a compromise draft of the Digital Services Act of November 2021 (DSA compromise draft)[257] for the first time implemented specific regulations on "dark patterns" for intermediary services, which were again significantly expanded and made more granular in the European Parliament's position of 20 January 2022 (DSA-EP)[258]. The provisions from the drafts have now been incorporated into Art. 25 DSA, but have been considerably toned down.

i. Online interface design and organisation, Art. 25 DSA

After a lengthy struggle, Art. 25 DSA and its Recital 67 created a provision that addresses online platforms for the design and organisation of online interfaces. This is the first substantive regulation on interface design in an act of secondary legislation that explicitly addresses "dark patterns", although they are not named as such.

According to Art. 25 (1) DSA, online platforms may not design, organise or operate their online interfaces in such a way that users are materially deceived, manipulated or otherwise significantly impaired or hindered in their ability to make free and informed decisions. While the prohibition of deception as behaviour that creates a gap between perception and reality can be considered comprehensible, the terms manipulation or other impairment of freedom of choice are very broad. It will therefore be important in the context of an interpretation of the provision in line with fundamental rights to interpret the term "materially" correctly. The mere influence that causes the user to reach different conclusions than they would have reached without influence cannot be sufficient on its own.[259]

In this respect, the literature is already endeavouring to fill out the characteristic and in doing so refers in part to the elements of the UCPD. *Dregelies* correctly chooses the approach that the characteristic is fulfilled if the average user cannot simply overcome the interference with the decision-making ability caused by the influence, but requires a certain amount of effort to allow the decision-making process to run smoothly.[260]

---

257 Available at: https://cdn.netzpolitik.org/wp-upload/2021/11/2021-11-15-conseil-dsa-approche-generale.pdf.

258 Available at: https://www.europarl.europa.eu/doceo/document/TA-9-2022-0014_EN.html.

259 Other opinion: *Martini/Kramme/Kamke*, MMR 2023, 323, 324, who state that causality of the influence would be constitutive here. On this, see also B. III. 2. above.

260 *Dregelies*, MMR 2023, 243, 246.

Art. 25 (2) DSA in turn considerably restricts the scope of application of the provision. It does not apply to practices that are already subject to the GDPR or the UCPD. As their scope of application in the digital environment is extremely broad, the question arises as to what scope of application should then remain for Art. 25 DSA. However, this is not a serious issue since – as shown – GDPR and the UCPD already provide a sharp sword for combating "dark patterns". Art. 25 DSA will therefore act as more of an appeal and provide a catch-all function. It is also conceivable that the guidelines that the Commission can draw up in accordance with Art. 25 (3) DSA will provide guidance for neighbouring areas of law. It remains to be seen what impact the provision will have in practice.

ii. Regulations for recommender systems, Art. 27 DSA

There is also a new provision for so-called recommender systems in Art. 27 DSA. Recommender systems are systems that are used by online platforms to suggest or prioritise certain information to users on their interface, including as a result of an initiated search, or that otherwise determine the relative order or prominence of the information displayed.[261] The regulation is thus reminiscent of new provisions introduced in UCPD with the Omnibus Directive,[262] which also regulates the display of search results and their ranking and which can constitute a *false hierarchy* pattern. The most striking difference is that Art. 27 DSA does not depend on whether the search order is sorted on the basis of a payment.

Providers of online platforms must state the most important parameters they use in their decision-making systems in clear and understandable language in their general terms and conditions and explain all options for users to change these parameters. If several options are available for recommender systems, the provider must also make a function available that allows the user to select and change their preferred option at any time.

c) Price Indication Directive

Special transparency obligations when trading with consumers also arise from the Price Indication Directive. In addition to new special features for the indication of price reductions,[263] the general rules also stipulate unambiguous, easily identifiable, and clearly legible price indications.[264] Since

261 Art. 3 lit. s DSA.
262 Art. 7 (4a) UCPD and Annex I No. 11a. See 2. a) and 2. c) above.
263 See 2. c) above.
264 Art. 4 (1) lit. c of the Price Indication Directive 2019/2161.

the purpose of the Directive is to better inform consumers and facilitate price comparisons,[265] there is much to suggest that it also includes indicating the prices in the respective national currency, which prevents *price comparison preventions* and *intermediate currencies*.[266]

6. Interim result

As can be seen, there are already numerous regulations in Consumer Contract Law, the UCPD and Data Protection Law that address and prohibit "dark patterns" to a large extent.

Hidden information patterns are countered by the provisions on Consumer Contract Law, which place high demands on the comprehensibility and completeness of the relevant information.[267] Art. 6 and Art. 8 UCPD can also be relevant if the customer has not been adequately informed and has been misled or aggressively influenced as a result.[268] Finally, Data Protection Law also requires informed consent, meaning that a declaration without transparently informing the data subject is ineffective.[269]

*False hierarch*y patterns are now addressed in online retail and marketplaces with No. 11a of Annex I of the UCPD and Art. 7 (4a) UCPD.[270] These do not prevent the controlled listing of products but make the ranking transparent for the consumer. If this is not sufficient, particularly manipulative *false hierarchies* can be prohibited via the general provision in Art. 5 (2) UCPD.[271] For companies falling under the scope of the DSA, Art. 27 DSA has a corresponding provision obliging providers of online platforms to provide the consumers with the relevant information on ranking results and even letting them configure their preferences.[272]

Countdown timers, *limited time messages* and *low stock/high demand messages* are already prohibited by No. 7 of Annex I UCPD if they exert sufficient pressure on the consumer due to the suggested scarcity or shortness of the offer time, as far as they are untrue. This leaves a small gap for cases in which no consequence of the expiration of the countdown is mentioned. In this case, the countdown is not objectively false and this No. 7 of Annex I UCPD is not applicable. However, this loophole can be closed *de lege lata* by Art. 6 UCPD, as a false consumer expectation might be

---

265 Art. 1 Price Indication Directive.

266 In Germany, the obligation to indicate prices in the national currency (EUR) falls under Section 1 (2) 2 of the national implementation of the Price Indication Directive (Preisangabenverordnung), see *Köhler*, in: Köhler/Bornkamm/Feddersen (eds.), 2024, Section 1 Preisangabenverordnung para. 21.

267 See 1. b) above.

268 See 2. b) and 2. c) above.

269 See 3. a) v. above.

270 See 2. b) and 2. c) above.

271 See 2. e) above.

272 See 5. b) ii. above.

created even without informing about the consequences of the expiry of a countdown, which might be misleading the consumer.[273]

Preselection is expressly prohibited in Art. 22 CRD, which also prevents *sneak into basket* patterns.[274] In Data Protection Law, *preselection* patterns are also prohibited by the requirement of expressing consent with a clearly confirming action and the "privacy by default" provision in Art. 25 (2) GDPR.[275]

Roach motel patterns are addressed by several regulatory complexes. Firstly, the right of cancellation means that in Consumer Contract Law it is generally possible to eliminate the consequences of a contract with retroactive effect.[276] Nevertheless, there are exceptions, for example if the trader immediately begins to fulfil the contract on digital products. In the case of data processing requiring consent, the right to revocation in Art. 7 (3) GDPR provides the possibility of preventing further data processing with future effect at any time.[277] Furthermore, in general, Art. 9 lit. d UCPD prohibits artificially complicating the termination of a contract.[278] This means that numerous instruments exist to counter *roach motel* patterns.[279]

Nagging can be regarded as an aggressive commercial practice above a certain level of persistence and is therefore prohibited under Art. 8 et seq. UCPD.[280] In addition, the "Privacy by Design" principle in Art. 25 (1) GDPR allows for the prohibition of harassing requests for consent.[281]

Forced registration patterns can – if the requirements are met – lead to ineffective consent under Data Protection Law.[282] *Hidden costs* patterns are prohibited under Consumer Contract Law and under No. 20 of Annex I of the UCPD.[283] *Disguised ads* patterns are addressed under No. 11a of Annex I of the UCPD, which prescribes the labelling of advertising in editorial content.[284] *Toying with emotion* patterns, such as *confirmshaming*, is so far only addressed as an aggressive business

273 See 2. c) above.
274 See 1. c) above.
275 See 3. a) vii. above.
276 See 1. e) above.
277 See 3. a) ix. above.
278 For the newly implemented cancellation button, making the termination of contracts easier, see III. 2. b) iii. below.
279 See 2. b) above.
280 See 2. b) above.
281 See 3. c) above.
282 See 3. a) above.
283 See 1. b) and 2. a) above.
284 See 2. a) above.

practice in exceptional cases.[285] Whether further prohibitions are necessary will be discussed below.[286]

Bait and switch patterns are addressed by Consumer Contract Law.[287] Furthermore Art. 6 et seq. UCPD prohibits misleading behaviour and can therefore also prevent *bait and switch* patterns.[288] In addition, No. 13 of Annex I of the UCPD prohibits a particular *bait and switch* pattern, namely the offering of imitation products under the pretence that they are the original.[289] Another particular *bait and switch* and *misdirection* pattern which is now subject to consent is the so-called *inbox advertising*.[290]

Recently, No. 23b and 23c of Annex I of the UCPD were implemented and also explicitly prohibit particular *social proof* or *testimonial* patterns.[291] This counteracts fake or purchased customer reviews.

Activity messages are not explicitly prohibited. However, they may be covered by Art. 6 et seq. UCPD,[292] as they can lead consumers to believe that there is a high demand for a good, which can lead to hasty purchasing behaviour. If necessary, the practice could also be addressed by Art. 5 (2) UCPD if they are not assumed to be misleading. *Hidden subscription* or *false continuity* patterns are prevented with the "button solution" in Consumer Contract Law[293] and No. 20 of Annex I of the UCPD, which prohibits to describe a product as "free of charge" if costs are nevertheless to be borne.[294]

Price comparison prevention and the special case of *intermediate currencies* are likely to contradict the provisions of the Price Indication Directive and are therefore already prohibited – at least in online retail.[295] Finally, *trick questions* patterns can be prohibited by Consumer Contract Law[296] or Art. 6 et seq. UCPD[297] as well as with the strong requirements of consent according to the GDPR[298] because they can be non-transparent or misleading.

---

285 See 2. b) above.
286 See III. below.
287 See 1. b) above.
288 See 2. c) above.
289 See 2. a) above.
290 See 5. a) above.
291 See 2. a) above.
292 See 2. c) above.
293 See 1. d) above.
294 See 2. c) above.
295 See 5. c) above.
296 See 1. b) above.
297 See 2. c) above.
298 See 4. a) viii. above.

As has been demonstrated, the practices identified in the study assessed by the EU Commission, as well as the practices identified by the CPC-network[299] for the sector of online retail are addressed to a very large extent by the existing legal framework. Nevertheless, not all practices are prohibited *per se*, but some are subject to additional conditions, such as the creation of a particular pressure situation or particularly aggressive behaviour. Other practices are not prohibited at all, but are subject to special transparency requirements, such as the labelling of advertising or the indication of how search results are ranked.

Recourse to the general clause in Art. 5 (2) UCPD is therefore only necessary *de lege lata* in exceptional cases, but is particularly useful if other practices emerge that appear to be worthy of prohibition. A major comprehensive *per se*-ban on "dark patterns", as is subject to occasional request, is therefore not necessary.

Finally, Consumer Contract Law,[300] the UCPD[301] and Data Protection Law[302] provisions also apply in principle if the trader or processor operates outside the EU.

According to the current status of the investigation, there seems to be no need for a comprehensive recreation of the legal framework to ensure digital fairness against the backdrop of "dark patterns".[303] In particular, there does not appear to be any need for abandoning the tried and tested model of the modern consumer. As it turns out for now, this model creates transparent and fair Consumer Law while preserving consumer sovereignty and is, as a rule, fit for the digital environment. Fundamental tightening, such as a departure from the modern consumer model, always carries the risk of a paternalistic image that cannot be reconciled with the idea of a sovereign consumer. Rather, at a first glance, it is advisable to carefully develop the current regulatory framework further in a principle based approach and on a case-by-case basis to create an evolution of consumer protection in the digital environment.

The introduction of so-called soft law would also be a conceivable solution. For example, a certification procedure led by the EU Commission or other authorities could be introduced. This would

---

299 See B. IV. 2. above.

300 See 3. a) above.

301 See 3. b) above.

302 See 4. d) above.

303 It should also be noted that the ECJ also takes a very consumer-friendly approach to the enforcement of consumer law. For example, it allows ex officio reviews of the effectiveness of jurisdiction or arbitration agreements in consumer law when examining the admissibility of an action (see inter alia *ECJ*, judgement of 27/6/2000, C-240/98-C-244/98; EJC, judgement of 6/10/2009, C-40/08).

allow traders who refrain from using "dark patterns" to be certified, which would increase consumer confidence in these traders. At the same time, the use of financial resources of consumer supervision could be spared by increasing the scrutiny of traders who do not use the certificate. In addition, the increased use of guidelines would also lead to greater legal certainty, especially in cases where dark patterns can only be addressed via general clauses.[304]

[304] See also III. 1. b) below.

III. Analysis of the reform proposals

Against the background of the results found, comprehensive reforms do not seem necessary. Should practices be identified that are worthy of prohibition, these can be banned by case law and official practice via general offences – and, if necessary, included by the legislator in Annex I of the UCPD. Nevertheless, the proposed reforms from the study assessed by the EU Commission and BEUC should be analysed below:

1. Proposals from the Commission study

The study assessed by the EU Commission rightly concludes that there is a strong framework of regulations in the EU that already effectively counters "dark patterns". Nevertheless, the researchers suggest selective tightening.[305]

a) Recommendations of the study

Firstly, they note that the current legal framework allows for grey areas in which it is unclear whether the behaviour is permitted or prohibited, which means that some, particularly compliant companies do not use practices, while other, more risk-taking companies do. The study also criticises inadequate enforcement. Since "dark patterns" lead to a "social dilemma", it is also worth considering whether a different distribution of the burden of proof or presentation should be considered in the event of digital asymmetries. It should be considered whether the retailer should not have to show that its commercial practices are fair and compliant.

The study also shows that transparency-based remedies are not efficient. The investigations show that such remedies would have no effect on consumer decisions. Rather, bans on the particularly harmful practices in Annex I of the UCPD or other provisions should be considered, as well as the creation of a fair/neutral design obligation for retailers. However, this should not only be ensured through regulatory measures, but also through guidelines and practical examples. The examples of behavioural taxonomy contained in the study can provide an indication of this.

---

[305] *Lupiáñez-Villanueva/Boluda/Bogliacino/Liva/Lechardoy/Rodríguez de las Heras Ballell*, Behavioural study on unfair commercial practices in the digital environment, 2022, p. 122 et seq., available at: https://op.europa.eu/en/publication-detail/-/publication/606365bc-d58b-11ec-a95f-01aa75ed71a1/language-en/format-PDF/source-257599418.

b) Evaluation

Most of the proposals in the study can be agreed with. Legal grey areas, as is inherent in open statutory regulations such as Art. 5 (2) UCPD, can create an unfair competitive environment in which some particularly cautious companies lose out while risk is rewarded. Although this is an acceptable dilemma in economic life within certain limits, it would be helpful for the functioning of the market if these grey areas were curbed. In this respect, it would make sense to clarify existing prohibitions through updated guidance to the UCPD by the authorities, so that the risk for users is more foreseeable, which would also create a fairer competitive environment. If this is not sufficient, it is possible in a second, stricter step to carefully integrate certain pracices into Annex I of the UCPD to increase legal certainty.

The study also addresses a very important point when referring to the lack of law enforcement. In the discussion about "dark patterns", the conclusion often seems to be drawn that there are too few prohibitions, which is why there are many "dark patterns". However, this might be a false conclusion and would be like stating that theft offences need to be reformed because theft continues to be committed. There is much to be said in favour that there are very powerful mechanisms of prohibition at the substantive law level. At first glance, enforcement therefore appears to be the main issue. So it seems that ways must be found to enforce the existing bans more effectively, be it more effective and efficient enforcement. To this end, it seems appropriate to review whether sufficient enforcement mechanisms are in place to ensure a fair and efficient level of enforcement at an appropriate level with adequate staffing and resources. If this is not the case, enforcement institutions would have to be expanded accordingly.

However, the aspect of modifying the burden of proof and presentation for traders seems problematic. Such regulations already exist in special situations, for example through the accountability obligation in Data Protection Law[306] or with the sale of consumer goods in view of the defectiveness of the item at the time of the transfer up to one year after receipt.[307] Usually, the purpose of reversing the burden of proof and presentation is to avoid having to provide proof of a fact that is either obvious or difficult for the claimant to demonstrate in the event of a dispute. Such regulations

306 Art. 5 (2) GDPR.
307 Art. 11 (1) Sales of Goods Directive.

are flanked by facilitations of proof in the procedural regulations of the member states.[308] A deviation from the general rule of presentation and burden of proof that the party who has to present and prove a fact that is favourable to him is therefore only sensible in such exceptional cases.

The creation of a different presentation and evidence regime is subject to high legitimisation pressure against the background of entrepreneurial freedom. On the one hand, this is due to the fact that even insufficient documentation can lead to the loss of a lawsuit if a judgement is made against a trader based solely on the rules of presentation and burden of proof. However, there are also secondary effects, such as increased compliance costs due to the permanent need to provide evidence of conformity, as every practice must be documented and retained as proof.

In any case, a general reversal of the burden of proof would only be justified if there are always problems of proof across the alleged "dark pattern" in a particular area. It is therefore doubtful whether a new allocation of the burden of proof would be proportionate against the background of entrepreneurial freedom with regard to the necessity of such provisions. A connection between the occurrence of "dark patterns" and a lack of evidence of compliance with consumer protection regulations is not discussed in detail in the study and not part of the discussion on that matter. It can therefore not be assumed that documenting compliance would lead to a higher level of consumer protection, but merely to a high financial burden for the companies concerned.

In addition, such a special case, as is the case with special rules on the burden of proof, is unlikely to apply with "dark patterns" *per se*. In general. it is not clear why the consumer or the person entitled to bring proceedings under the UCPD should have specific difficulties in providing evidence against traders which use "dark patterns". The use of most of the online practices, such as those discussed in the study, makes it particularly easy to being documented, for example by taking screenshots. In cases where such screenshots do not explicitly show hidden modes of the operation of "dark patterns", such as how algorithms are designed to trigger influencing mechanisms, the existence of mere indications should be sufficient to impose a secondary burden of presentation and proof on traders, even under the current legal situation. Then the traders have to show the technical design of the interface. This applies all the more if Data Protection Law is applicable, as

[308] For example, the so-called "secondary burden of presentation and proof" in German Law, according to which a de facto reversal of the burden of proof exists in extreme exceptional cases if the claimant cannot provide the proof himself, but it seems appropriate for normative reasons that the opponent may be burdened with proof, since it is closer to the evidence and it can be expected of him to provide the proof.

the accountability obligation under Art. 5 (2) GDPR takes effect and leads to a de facto (situational) reversal of the burden of proof.[309]

In principle, therefore, there is no need for new rules of evidence. As an exception, difficulties of proof, which could then be legally resolved, may exist in cases in which the unfairness of a behaviour stems from facts that are beyond the consumer's knowledge. This can be the case, for example, with *scarcity* and *activity messages* patterns, as the truth of the shortage or the behaviour of other users is relevant for the classification as unfair. In these individual cases, it might be conceivable, for example, to impose simple corresponding documentation obligations on traders using such patterns to prove how they ensure the accuracy of the information.

2. BEUC proposals

BEUC also provides concrete reform proposals to counter "dark patterns" and to tighten up the legal framework for digital fairness.[310]

a) Recommendations

In BEUCs assessment, important mechanisms exist to protect consumers from "dark patterns", but regulation falls short given the scale and widespread nature of the phenomenon. BEUC therefore proposes amending the UCPD with a new concept of digital asymmetry and digital vulnerability in commercial behaviour and a general concept of "fairness by design" which should transfer principles known from GDPR into Consumer Law. Exploitation of digital asymmetry should constitute a material impairment under the UCPD. A duty of care should be implemented to ensure that the consumer's freedom of choice is not impaired by the commercial practices, in particular by the design and operation of an interface. This should apply to all cases where digital asymmetry increases the risk of material behavioural bias, in particular algorithmic personalisation of choice architectures, behavioural profiling for commercial purposes or recommendation environments where bias or vulnerability could be identified, reinforced or created. In addition, digital vulnerability as a universal state of susceptibility should be added to the recitals of the UCPD. The recitals

309 See II. 3. b) above.

310 *BEUC*, "Dark Patterns" and the EU Consumer Law acquis, p. 13, available at: https://www.beuc.eu/sites/default/files/publications/beuc-x-2022-013_dark_patters_paper.pdf, EU Consumer Protection 2.0, p 8 et seq., available at: https://www.beuc.eu/sites/default/files/publications/beuc-x-2022-015_protecting_fairness_and_consumer_choice_in_a_digital_economy.pdf, *Helberger, Kas, Micklitz, Namyslowska, Naudts, Rott, Sax, Veale*, Digital Fairness for Consumers, 2024, available at: https://pure.eur.nl/ws/portalfiles/portal/139212255/BEUC-X-2024-032_Digital_fairness_for_consumers_Report.pdf, p. 262 et seq.

should indicate digital asymmetry resulting from either structural difference in the power to influence the process of autonomous decision making of the other party, the control over data or the architecture of the digital choice environment. Furthermore, digital asymmetry that result of imbalances in the commercial relationship that a digital B2C environment creates and maintains or of situations of imbalance in relation to the knowledge and understanding of the functioning and impact of a digital commercial practice should be included in the recitals to the UCPD. Moreover, BEUC is in favour of a right of recourse for traders in the UCPD if the trader is held liable for a breach due to unlawful data or due to a data collection structure over which the trader has no control and with which data was collected in an unlawful manner.[311]

BEUC also proposes amending the CRD with an obligation to have a contract cancellation button, making the cancellation of a contract as easy as the agreement to enter into it. Moreover, BEUC proposes to create an obligation to interface neutrality where appropriate and to include certain practices in Annex I of the UCPD. This relates in particular to the phenomenon of *confirmshaming*. According to BEUC, it is also important that consumers have access to individual remedies, such as the termination of a contract if it has been concluded on unfair terms.

Finally, BEUC also calls for a reversal of the burden of proof. It is said to be disproportionately difficult for the consumer to prove the digital asymmetry, while it should be easy for the trader.

b) Evaluation

In the following, the BEUC proposals will be discussed in detail:

i. A new concept of "digital asymmetry", "digital vulnerability" and "unfair digital commercial practices"

The need to implement a comprehensive concept of digital asymmetry seems doubtful. After all, Consumer Law as a whole is based on the idea of the structural inferiority of the consumer compared to the trader. It is therefore questionable whether the acknowledgement of a general digital asymmetry or digital vulnerability adds relevant new aspects or is rather *old wine in new bottles*.

As a rule, it must be noted that consumers in the online environment can sometimes be more susceptible to influence due to easier possibilities of digitalisation, including personalisation. However, this must be countered by the fact that consumers have numerous advantages in the digital

311 *Helberger, Kas, Micklitz, Namyslowska, Naudts, Rott, Sax, Veale*, Digital Fairness for Consumers, 2024, available at: https://pure.eur.nl/ws/portalfiles/portal/139212255/BEUC-X-2024-032_Digital_fairness_for_consumers_Report.pdf, p. 267 et seq.

environment. For example, there is a consumer cancellation right in distance selling. In addition, particular transparency obligations apply that are intended to compensate for any lack of knowledge on the part of the consumer. Consumer Contract Law ensures that consumers benefit of a high level of their protection online, which should significantly reduce any asymmetries with traders. In addition, as a rule, consumers in the online environment have the advantage of being able to easily document websites so that deceptions or other manipulations can easily be proven. Finally, digital assistants, such as price comparison portals, can also lead to special advantages for consumers on the Internet. Against the background of the European consumer model of an average consumer, it therefore does not seem appropriate to assume a digital asymmetry or digital vulnerability *per se* and across the entire online sector.

Against this background, the necessity of introducing a special offence of "unfair digital commercial practice" and a second general clause for such practices also seems doubtful.[312] This presupposes a parallel regulatory regime in addition to the proven and broadly defined core provisions of the UCPD, whereby, as shown, the existing digital practices can be addressed under the offences of the UCPD after appropriate interpretation, otherwise via other regulatory frameworks. The introduction of a second general clause analogous to Art. 5 (2) UCPD, in which existing terms are used that are merely supplemented by the word 'digital', is more likely to create legal uncertainty, as there are difficulties in drawing a distinction with the other provisions.

Should the legislator nevertheless opt to achieve such legislation, it would probably have to deviate from the prevailing modern consumer model and adopt a more paternalistic consumer model. This is, in principle, permissible when rightfully weighing up the conflicting interests, such as that of entrepreneurial freedom, finely and carefully and balance the principles and fundamental rights of all those affected.[313] It is the legislator's prerogative to assess whether such an approach is necessary. However, given that the identified practices are already sufficiently addressed by Consumer and Data Protection Law *de lege lata*, there are justified doubts as to the necessity of such a measure.

---

312 *Helberger, Kas, Micklitz, Namyslowska, Naudts, Rott, Sax, Veale*, Digital Fairness for Consumers, 2024, available at: https://pure.eur.nl/ws/portalfiles/portal/139212255/BEUC-X-2024-032_Digital_fairness_for_consumers_Report.pdf, p. 269 et seq.

313 See I. 1. d) above.

ii. A new concept of "fairness by design" and "interface neutrality"

Another BEUC proposal envisages the implementation of a "fairness by design" obligation, analogous to Art. 25 GDPR. A critical aspect of such a proposal is that such offences create a high degree of legal uncertainty, which is already a concern with Art. 25 GDPR.[314] Therefore, there are also doubts about the necessity of such a provision, as it would hardly bring any concretisation benefits beyond the general clause in Art. 5 (2) UCPD. Should the legislator decide to create such an obligation, it is advisable to provide guidance on maintaining fair standards so that traders can be compliant.

The proposal on "interface neutrality" also raises concerns. After all, the interface of an online shop is its main source of communication with the customer. In addition to the website's offering, the way in which users experience the website also creates value for the trader by creating recognition and character of their website. Therefore, regulations concerning the design of the interface in a completely neutral way are likely to represent a profound encroachment on the entrepreneurial freedom and, if applicable, also on the freedom of communication of traders. Again, such an obligation is likely to not follow from the modern consumer model. Obligations to establish a neutral design are more likely to require a more paternalistic consumer model.[315]

iii. A "contract cancellation" button

The cancellation button has firstly been implemented in Germany in Consumer Contract Law[316] and was implemented for distance contracts on Union level in November 2023,[317] to be transposed by the Member States in December 2025.[318] The German implementation has been met with particular concerns about abuse, as it makes it possible to simply cancel third-party contracts without identification (e.g. through a customer account).[319] It was therefore argued at an early stage that the provision of a cancellation email address should be made mandatory.[320] Great care must therefore be taken to ensure that the precise implementation of any "contract cancellation" button or function does not render the function open to abuse.

---

314 See II. 3. c) above.
315 See i. above.
316 Para. 312k BGB.
317 See Art. 1 (3) Directive 2023/2673, amending the CRD with Art. 11a.
318 Art. 2 Directive 2023/2673.
319 See *Maume*, in: Hau/Poseck (eds.), 2023, Section 312k BGB para. 6 et seq.
320 *Maume*, in: Hau/Poseck (eds.), 2023, Section 312k BGB para. 6 with reference to *Güster/Booke* MMR 2022, 452.

iv. A right of recourse for traders that purchased data or data collected by external mechanisms

Another interesting concept is the proposal to implement a right of recourse for traders who have purchased or collected data from a third-party not controlled by the trader and the processing has turned out to be unlawful. In this case, if appropriate verification mechanisms are in place, the proposal is that there should be a right of recourse to the originator of the data, which should be implemented in the UCPD.[321] This is based on the fact that data protection violations can also be asserted by competitors or associations in the context of UCPD proceedings, which is why there is a need for recourse by traders against third-parties.[322]

Even though this is an interesting proposal, it is a very specific provision that regulates individual cases. Such a right of recourse is otherwise foreign to the UCPD, which is why it is questionable why such a right should be regulated in the UCPD, especially in the case of the use of unlawfully collected data. It is therefore questionable whether it needs to be included in a cross-sectoral law such as the UCPD. On the other hand, there is much to suggest that a right of recourse must be resolved via contract law, whereby such a right often already exists in the contractual relationship between the trader and the third-party. It is likely that the general liability for material defects applies in such cases. Therefore, it is questionable whether there is actually a need for such a statutory provision.

v. New rules on the burden of proof

As already stated,[323] the reversal of the burden of proof and presentation typically aims to circumvent the need to provide evidence for a fact that is either self-evident or challenging for the claimant to demonstrate in case of a dispute. Such provisions are complemented by procedural facilitations of proof within the member states. Against the backdrop of enormous compliance challenges, a departure from general rules on the burden of proof is therefore likely to depend on the existence of such a situation to be proportionate.

However, it is not clear why such a situation should be applicable with "dark patterns" *per se*. It is not evident to what extent it should be particularly difficult to document and prove unfair practices by traders in the online sector. On the contrary, gaining proof should be much easier compared to

---

321 The proposal is similar to Art. 20 Directive 2019/770

322 *Helberger, Kas, Micklitz, Namyslowska, Naudts, Rott, Sax, Veale*, Digital Fairness for Consumers, 2024, available at: https://pure.eur.nl/ws/portalfiles/portal/139212255/BEUC-X-2024-032_Digital_fairness_for_consumers_Report.pdf, p. 267 et seq.

323 See 1. b) above.

offline-trading due to the possibility of screenshotting, the browser history, archive databases with scans of older websites etc. at any time.

In the event that there is a suspicion that an interface is personalised, this presupposes the processing of personal data, so that Data Protection Law is applicable. In order to find out whether an interface is personalised at all, Art. 15 (1) GDPR gives the data subject the right to ask whether personal data is being processed. If the request is positive, and personal data is processed, there is an accountability obligation *de lege lata* with Art. 5 (2) GDPR, which leads to a de facto reversal of the burden of proof for the data processor.[324] A tool therefore already exists for personalisation processes that cannot be proven by the consumer so that they do not have to explain and prove a corresponding personalisation practice and its challenges in a legal process.

Against this background, a blanket reversal of the burden of proof is unlikely to be proportionate according to the current state of the investigation. Specific situations in which there is a difficulty in providing evidence, but which still need to be addressed, could lead to a different assessment. However, even in such cases, the reversal of the burden of proof should not be the only conceivable means of addressing the problem so that other, less intrusive measures will also need be examined. Against this background, it is to be welcomed that the more recent report commissioned by BEUC is more cautious.[325] It proposes to include a clause according to which, following the submission of facts and evidence by the plaintiff that sufficiently prove an unfair commercial practice, it is up to the trader to provide evidence to the contrary. This is in fact a codification of the so-called "secondary burden of presentation and proof".[326] After a rather detailed elaboration of various possibilities,[327] this balances the facilitation of evidence for plaintiffs on the one side and the protection of the interests of traders on the other side, which at the same time prevents the plaintiff from being released from any burden of proof, which could be used in an abusive manner. It is also to be welcomed that a clause is to be included according to which business secrets are to be protected. If it turns out that these procedures do not already exist under the legal systems of the Member States, there is a case for including such a provision in the UCPD.

---

324 See II. 3. b) above.

325 *Helberger, Kas, Micklitz, Namyslowska, Naudts, Rott, Sax, Veale*, Digital Fairness for Consumers, 2024, available at: https://pure.eur.nl/ws/portalfiles/portal/139212255/BEUC-X-2024-032_Digital_fairness_for_consumers_Report.pdf, p. 277 et seq.

326 See 1. b) above.

327 *Helberger, Kas, Micklitz, Namyslowska, Naudts, Rott, Sax, Veale*, Digital Fairness for Consumers, 2024, available at: https://pure.eur.nl/ws/portalfiles/portal/139212255/BEUC-X-2024-032_Digital_fairness_for_consumers_Report.pdf, p. 242 et seq.

vi. Implementation of further practices in Annex I of the UCPD

This study indicates that Annex I of the UCPD is a suitable tool in the fight against "dark patterns".[328] It explicitly prohibits practices, which generally ensures a high degree of legal certainty and fair market conditions between companies. BEUC is therefore right that further offences that are to be prohibited should primarily be included there. The "dark pattern" *confirmshaming* in particular is to be included.

In general, the need for such a ban can be understood as *confirmshaming* a certain degree of effectiveness.[329] However, it must be taken into account that such patterns are already prohibited if they occur as an aggressive practice.[330] A *per se* ban on emotionally influencing the buyer would mean a very far-reaching encroachment on the entrepreneurial freedom and possibly the freedom of communication of online retailers. After all, they are primarily dependent on their design to create emotions, which is a prerequisite for customer relationships. A certain "Wouldn't you like to stay after all?" in the event of cancellation might be considered an appropriate question for a trader if it does not want to lose customers. On the other hand, politeness sometimes requires that customers are addressed emotionally, such as with a "We miss you" in a newsletter. Such statements that express appreciation for the customer are sometimes even expected. There are also likely to be major cultural differences as to whether such an approach to customers is considered polite and expected accordingly in the individual Member States, or whether it is perceived as aggressive and annoying and triggers a need for prohibition. It must therefore be noted that companies have a legitimate interest in inducing and reinforcing positive connections in their communication with costumers. A general ban on *confirmshaming* in Annex I of the UCPD would therefore prohibit practices that also fall under acceptable everyday communication. This could also be associated with legal uncertainty, as it is difficult to determine which approach triggers emotions and which does not.

It can therefore be assumed that the legal means already provided with the UCPD on aggressive business practices are sufficient to counter the phenomenon, which requires a certain degree of flexibility in handling. Against this background, the call for a comitology procedure for Annex I

---

328 See II. 2. a) above.

329 See *Lupiáñez-Villanueva/Boluda/Bogliacino/Liva/Lechardoy/Rodríguez de las Heras Ballell*, Behavioural study on unfair commercial practices in the digital environment, 2022, p. 98 et seq, available at: https://op.europa.eu/en/publication-detail/-/publication/606365bc-d58b-11ec-a95f-01aa75ed71a1/language-en/format-PDF/source-257599418.

330 See II.2. b) above.

UCPD[331] seems understandable. However, it must be taken into account that the democratic legitimisation of prohibitions must be safeguarded, particularly in view of the strong sensitivity of this area to fundamental rights. In view of the great flexibility that the legislator has demonstrated in the ordinary procedure in recent years, it is unclear whether implementing a comitology procedure is necessary in order to be able to react quickly and flexibly. This is particularly true in light of the fact that legal certainty can also be achieved through soft law, for example in the form of guidelines, and enforcement can be based on general offences such as 5 (2) UCPD.

331 *Helberger, Kas, Micklitz, Namyslowska, Naudts, Rott, Sax, Veale, Digital Fairness for Consumers, 2024, available at: https://pure.eur.nl/ws/portalfiles/portal/139212255/BEUC-X-2024-032_Digital_fairness_for_consumers_Report.pdf, p. 276*.

D. Results

The study led to the following results:

1. Recently, the term "digital fairness" has been increasingly discussed in the context of the regulation of consumer protection rights. In particular, the focus has been on investigations into designs that aim to manipulate consumers. For these practices, "dark patterns" has become a buzzword. However, influencing consumers is far from new and is a traditional approach for companies. After all, even simple advertising seems unnecessary if it is not intended to stimulate – i.e. influence – the addressee to consume.

Digital fairness and "dark patterns" in the focus of the EU Commission

2. In the context of the EU Commission's initiative to review the consumer rights framework for "digital fairness", "dark patterns" have therefore recently been in the news. A study assigned by the EU Commission found numerous "dark patterns", some of which were also found in the online retailing. A sweep by the CPC network, specifically for online shops and marketplaces, found an even higher hit rate.

   Not surprisingly, the overarching theme of the studies, "digital fairness", quickly leads to the area of "dark patterns". Although "digital fairness" is a broad field, the current discussion in the online B2C sector outside of Data Protection Law is almost exclusively limited to this specific topic, which is discussed in particular against the background of Consumer Contract Law and the UCPD.

Difficult definition of the term "dark patterns"

3. The term "dark patterns" is difficult to define, as it stands for influencing practices in a constantly evolving environment. It seems quite clear that "dark patterns" are to be used in the communication with consumers because of their particular vulnerability due to attention or rationality deficits. However, the characterising attribute of having an influencing effect already shows that it is not easy to distinguish between acceptable influence and *dark* manipulation. One possible demarcation criterion is that a "dark pattern" exists if its influence leads to a consumer decision that is not supported by their actual will.

4. However, it is particularly important that the consumer influence is all in the traders' interests. This also distinguishes it from a simple nudging of the consumers' decisions in a certain direction. The term nudging sometimes has a rather positive connotation, as it is used for practices steering consumers towards advantageous behaviour. On the other hand, this cannot hide the fact that whoever uses nudging practices might also indirectly unilaterally enforce their own interests. One example of this is greenwashing, which (only partially) leads to consumers being steered towards environmentally friendly behaviour, whereas the traders' interests are at the forefront. For the definition of "dark patterns" it must therefore be irrelevant whether the influence pursues other (possible) interests, such as public welfare or environmental interests, as long as the influence (also) serves the trader.
5. Although the term "dark patterns" is used particularly in the context of online B2C, this is by no means obligatory. There are also many practices in the "offline" world that can be qualified as "dark patterns".
6. In the end, it is important to bear in mind that categorising a phenomenon such as a "dark pattern" alone is not sufficient to classify a practice as worthy of being prohibited, partly due to the rather vague definition. Therefore, the qualification of a practice as a "dark pattern" does not exempt it from a legal investigation into the possibility of a prohibition *de lege lata*, nor, in the case of legislative proposals, from an impact assessment into whether it is worthy of a prohibition.

Examination of the studies examples on "dark patterns" for their relevance in online retail

7. The practices identified with the sweep by the CPC Network cannot be analysed for their relevance due to the absence of individual examples. On the other hand, an examination of the practices from the study assigned by the EU Commission shows numerous examples, many of which seem problematic and show that "dark patterns" have a certain prevalence in online retail. However, many of the practices are particularly relevant for other sectors such as social networks. Furthermore, with some individual examples, a classification of the practices as "dark patterns" appears doubtful. For this reason, some of the examples for the online retail sector can be filtered out as irrelevant, which reduces the total number of cases found.

Fundamental rights framework for regulations on "dark patterns"

8. When revising provisions on "dark patterns", the legislator is faced with a difficult conflict of various fundamental rights. On the one hand, as a rule, traders and their business models are protected by the entrepreneurial freedom. On the other hand, the trader's freedom of communication may also be taken into account. However, case law allows quite far-reaching interventions in entrepreneurial rights for the purpose of consumer protection, which means that further regulations on "dark patterns" are possible provided that the interventions are proportionate. To determine the necessary level of consumer protection, the legislator currently uses the model of the reasonably informed and reasonably attentive average consumer – also known as the modern consumer model. It takes this into account when creating new Consumer Law provisions and it represents a balance between protective paternalism and economic liberalism. In addition, the legislator had entrepreneurial freedom in particular in mind, which it wanted to harmonise with consumer protection when it created the modern consumer model. If the legislator wishes to continue to apply the modern consumer model, a certain degree of influence on the consumer must be accepted, as the consumer is given a certain degree of responsibility. However, in addition to the obligation to provide a high level of consumer protection, the fundamental right to data protection must also be harmonised with entrepreneurial freedom by achieving a solution that ensures a gentle balance between the competing fundamental rights and principles.

Requirements for proof of practice for bans

9. In the context of creating new legislation, the question also arises as to what evidence the legislator must have of the existence of a particular practice in order to be able to prohibit it. The case law of the European Court of Justice grants the legislator a wide margin of discretion in this respect. However, this has been criticised for good reasons, since the burden of proof for the necessity of a burdensome regulation lies with the subject of the fundamental right. Against this background, there is much to suggest that the more burdensome a rule is for a subject of fundamental rights, the higher the level of evidence must be. For example, rules that trigger particularly high compliance requirements must be justified and proven to a greater extent than those that are easy to implement and less intrusive. Against this backdrop, there are some indications that the evidence from the EU Commission's study is not sufficient to justify far-reaching bans on "dark patterns" in the online retail sector.

The trade-off between sector-specific law and opaque fragmentation

10. It should be noted that the legislator can, within certain limits, create specific sectoral legislation, which would have the advantage of prohibiting only those practices in the sectors in which they actually occur. This would be particularly protective of fundamental rights for companies operating in other sectors. However, this must not lead to the creation of a conflict-laden interplay of different legal acts, some of which overlap and whose complicated demarcation leads to legal uncertainty, as can be observed in some areas of digital law. On the other hand, as Consumer Contract Law and the UCPD already make sectoral distinctions within the respective regulatory frameworks, the risk of such fragmentation with demarcation difficulties is rather low.

Consumer Contract Law addressing "dark patterns"

11. In the subsequent assessment of the legal framework, Consumer Contract Law which is laid down in particular in the CRD had to be addressed first. It has numerous transparency requirements, so that such particular types of "dark patterns" which rely on the concealment of information are effectively prohibited. In addition, there is also a prohibition of default settings, which prohibits *snitch into basket* and *preselection* patterns. The "button solution" and certain transparency requirements in the e-commerce sector also increase transparency in this area and prevent patterns that rely on the concealment of information.
12. This is supplemented by extensive cancellation rights, which – with a few exceptions – provide an easy way to eliminate undesirable contractual effects without having to justify the cancellation. The new Sale of Goods Directive also contains further transparency obligations, so that overall, it can be seen that the Consumer Contract Law already prohibits a large proportion of "dark patterns".

Numerous rules on "dark patterns" in the UCPD

13. In the UCPD numerous "dark patterns" are prohibited in Annex I. These are per se prohibitions, i.e. practices that are always prohibited without further scrutiny. These include *false countdown* patterns, *disguised ads* patterns, certain types of *false hierarchy* patterns, a type of *misdirection* pattern and a type of *hidden costs* and *hidden subscription* patterns. The *social proof* pattern of purchased or falsified customer reviews is also addressed in Annex I of the UCPD.

14. In addition, numerous "dark patterns" can also be qualified as aggressive commercial practices which are prohibited by Art. 8 et seq. of the UCPD. These include *nagging* and *click-fatigue* patterns. The *roach motel* pattern is also explicitly mentioned there. Furthermore, *toying with emotion* patterns such as the *confirmshaming* pattern can also be subsumed under the provisions in individual cases of particularly aggressive behaviour.
15. The offence of misleading action in Art. 6 et seq. UCPD is also relevant for "dark patterns". For example, *countdowns*, *scarcity* patterns or *activity messages* can be prohibited if they can have a misleading effect on the consumer. *Hidden information* and *misdirection patterns* also fall under this standard. There is also a special provision for particular types of *false hierarchy* patterns and *social proof* patterns. In addition, there is numerous case law according to which *bait and switch* patterns are prohibited under Art. 6 et seq. UCPD.
16. If the special conditions of the UCPD do not apply, it is possible to fall back on the catch-all clause in Art. 5 (2) UCPD. This can already be used, for example in the event of the occurrence of previously unaddressed "dark patterns" if they are materially influencing the customer in an unjustified way.

Effective law enforcement also for traders outside the EU

17. The Rome I and Rome II Regulations contain provisions that stipulate that the provisions of Consumer Contract Law and the UCPD also apply if a trader based outside the EU at least directs its business activities to consumers in Member States of the Union or if this has effects on the collective interests of consumers in a Member States or the EU. It can therefore be assumed at first glance that traders outside the EU are also effectively subject to the provisions and that there is therefore no legal gap in consumer protection in these scenarios. Nevertheless, there might be an enforcement gap.

GDPR and "dark patterns"

18. Data Protection Law, which is characterised by numerous general terms, can also address "dark patterns". In the context of consent, this is particularly the case for the prerequisite of voluntariness, as well as for the necessity of a clearly confirming action, which can prevent *preselection* or *forced registration* patterns.
19. Consent as an instrument for ensuring digital sovereignty is therefore an effective means of ensuring that consent corresponds to the will of the data subject through a variety of carefully

balanced mechanisms. It is therefore surprising that a BEUC study concluded that a large number of data subjects surveyed consider data processing for monetisation or analysis to be unfair. This could be since the mechanisms of consent may not be effectively enforced in practice. In any case, it should be noted that monetisation in data-driven business models is what makes it possible to finance the services in the first place. In cases where the requirements for consent are met, i.e. consent is given voluntarily due to other market alternatives, this should therefore not be seen as unfair per se. After all, the service must be financed somehow. To ensure that consent is voluntary, "pay or okay" models may be used here, in which the data subject has the choice of using the service or parts of it for a fee or in exchange for the processing of personal data. This practice was recently approved in principle by the ECJ. Nevertheless, it seems doubtful whether there is sufficient legal enforcement, which makes it more understandable that data subjects consider data processing to be unfair.

20. If there are personalised "dark patterns", the accountability provision in Art. 5 (2) General Data Protection Regulation (GDPR) leads to a reversal of the burden of proof and thus makes it easier for data subjects to enforce their rights. In addition, the transparency requirements also ensure that *hidden information* patterns are prevented. Furthermore, the regulations on privacy by design and privacy by default can be used to ensure a fair environment. However, this has not yet been sufficiently specific and requires further clarification such as a guidance by the Data protection authorities. An effective enforcement is therefore doubtful.
21. In addition, it has also been shown that the market location principle means that legal enforcement for data protection violations committed by processors outside the EU is also subject to the efficient regulatory regime of the GDPR. Here again it is important to have an effective enforcement of the existing rules.

Specific provisions on "dark patterns" in other legal areas

22. Finally, there are other areas in which "dark patterns" are addressed. A judgment by the European Court of Justice now only permits inbox advertising, i.e. the display of advertising in an email list, which is a *bait and switch* and *misdirection* pattern, with the consent of the user. Labelling it as advertising alone is no longer sufficient. Art. 27 DSA contains a provision for online platforms, according to which they must explain how search results are obtained and, if

necessary, even allow consumers to adjust their settings. This addresses *false hierarchy* patterns. Finally, the Price Indication Directive is aimed at price transparency and facilitating price comparisons which prevents *interim currency* and *price comparison prevention* patterns.

Comprehensive coverage of relevant "dark patterns" in the current legal framework

23. According to the current status of the investigation, there are many indications that the practices listed by the CPC Network and in the EU Commission's study are covered by the current legal framework to a large extent:

24. *Hidden information* patterns are effectively prevented by the transparency requirements of Consumer Contract Law and, where applicable, Art. 6 and 8 of the UCPD and Data Protection Law. *False hierarchy* patterns are addressed in numerous new provisions and ensure that the criteria that lead to a certain ranking must be communicated transparently. If this turns out to be not sufficient in individual cases, the pattern can be prohibited via Art. 5 (2) UCPD. *Countdown timers* and *limited time messages* as well as *low stock/high demand* messages are already partially prohibited by Annex I UCPD. Any gaps in protection can be closed with Art. 6 UCPD. *Preselection* patterns are prohibited by the ban on default settings in the CRD and the GDPR. *Roach motel* patterns are sanctioned by the right of cancellation, the right to revocation in Data Protection Law and – if the exercise of rights is artificially impeded – by Art. 9 lit. d UCPD. *Nagging* falls under aggressive commercial practice above a certain threshold and is therefore prohibited under Art. 8 et seq. UCPD. "Privacy by design" according to Art. 25 GDPR can also lead to such a ban. *Forced registration* patterns can be prohibited with the requirements of consent under Data Protection Law. *Hidden costs* patterns are addressed by the transparency requirements in Consumer Contract Law and Annex I of the UCPD. *Disguised ads* patterns are also prohibited by Annex I of the UCPD. *Toying with emotions* patterns, such as *confirmshaming*, can be prohibited in exceptional cases as aggressive business practice under the UCPD. *Bait and switch* patterns are prohibited under the provisions of Consumer Contract Law and the prohibition of misleading advertising in the UCPD. A special *bait and switch* pattern, namely the offer of fake products under the impression that they are originals, is explicitly prohibited under Annex I of the UCPD. Inbox advertising, a particular *bait and switch* pattern, is prohibited by the ePrivacy Directive according to a recent judgment of the European Court of Justice.

25. Certain *social proof* patterns are now also prohibited by Annex I of the UCPD. These are patterns that consist of fake or purchased customer reviews. *Activity messages* are not expressly prohibited, but can be misleading – in line with *scarcity* patterns – or might be prohibited under Art. 5 (2) UCPD when materially distorting the consumer. *Hidden subscription* and *false continuity* patterns are countered with the "button solution" in Consumer Contract Law. Annex I of the UCPD also provides for a ban on labelling a product as free if costs are actually incurred, which also addresses a particular *hidden subscription* and *hidden costs* pattern.
26. Price *comparison prevention* and *intermediate currencies* are likely to be prohibited by the provisions of the Price Indication Directive. Finally, *trick question* patterns may also be prohibited under Consumer Contract Law, fall under the UCPD as misleading, or can be dealt with in the context of privacy consent requirements.
27. The prevalence of numerous "dark patterns" revealed in the investigations, such as those assigned by the EU Commission or the CPC Network sweep underscores a deficiency in law enforcement mechanisms. As demonstrated, comprehensive regulations addressing "dark patterns" already exist, rendering the creation of further rules necessary only for addressing specific details.
28. Based on the results, only minor adjustments to the regulatory framework seem necessary, while the focus should be on using existing mechanisms for effective law enforcement. In addition, the implementation of soft law can also be considered, for example through the provision of guidance by the competent authorities or the introduction of certificates for compliant traders.

Review of reform proposals on digital fairness and "dark patterns" in the EU Commission study

29. It can therefore be seen that the practices identified by the EU Commission study and the CPC network are already prohibited *de lege lata* or at least addressed. Against this background, the reform proposals from the study by the EU Commission and the consumer organisation BEUC had to be examined.
30. The EU Commission's study initially proposes closing grey areas. This can be achieved by ensuring legal certainty by including inadmissible practices in Annex I of the UCPD where possible or at least providing guidance from authorities or organisations on the interpretation

of open legal terms. The study also underlines – as does this legal opinion – that there is rather a lack of law enforcement than a lack of an effective regulations on "dark patterns".

31. However, the proposal to create a new comprehensive shift in the burden of proof is to be rejected. Reversals of the burden of proof only exist in narrow exceptional cases. Such an exceptional case does not exist in the area of B2C online business *per se*. A general lack of provability for the consumer is particularly difficult to imagine, as the ability to take screenshots and precisely document processes is particularly good in the online sector and relevant in most cases of "dark patterns". However, difficulties of proof are conceivable in cases where the fairness of a pattern is based on facts outside of the perception of the consumer, for example in the case of *scarcity* or *activity message* patterns. Here, the truthfulness of the assertions, for example whether the goods are indeed scarce or whether other consumers are indeed looking at the offer, is relevant for a categorisation as a "dark pattern" and at the same time hard for the consumer to prove. In such special cases, it seems conceivable to impose documentation obligations on traders who use such mechanisms to ensure that the information is correct. In any case, any changes with respect to the burden of proof would need a clear identification of specific situations in which the consumer is not able to present evidence. And again, any new rule created should be enforced effectively afterwards.

Review of reform proposals on digital fairness by BEUC

32. Next, the BEUC proposals were to be examined. BEUC proposes the general implementation of a new concept of digital asymmetry,digital vulnerability and digital commercial practice. There are well-founded concerns as to whether this is necessary, as the asymmetry of consumers and traders is already at the heart of Consumer Protection Law, so it cannot be assumed that the current situation does not adequately address asymmetry. After all, numerous disadvantages that consumers have are already compensated for by special transparency requirements and easier cancellation options for contracts. In particular, the introduction of a second general clause for digital commercial practices does not appear sensible, as it would create difficulties in drawing a distinction with the general clause, especially as the known cases of manipulative techniques are already sufficiently addressed by the existing provisions. Should the legislator consider implementing a corresponding concept, this would probably require a departure from the current model of the modern consumer in favour of a more paternalistic Consumer Law approach. In doing so, the legislator would have to weigh up the conflicting

interests, such as that of entrepreneurial freedom, finely and carefully and balance the principles and fundamental rights of all those affected. Moreover, legal certainty is of paramount importance. Thus, any new rule has to be as precise as possible in order to be enforced effectively.

33. BEUC also proposes the introduction of fairness by design and interface neutrality. Fairness by design is to be adopted from the principle of privacy by design from the GDPR. This raises concerns, as the privacy by design principle is dependent on further interpretation and is therefore hardly suitable as a benchmark. Corresponding requirements could also already be solved with the general clause in Art. 5 (2) UCPD, which nevertheless has the disadvantage of only little prior structuring and thus increased legal uncertainty. In any case, guidance from the responsible supervisory authority would be advantageous.
34. There are also legal concerns about regulating the interface. The obligation to design the interface of a website or app neutrally prohibits companies from giving their web presence recognition value and character, which – in addition to the goods and services offered – creates value for the company. An obligation to design the interfaces in a completely neutral way is therefore likely to represent a profound encroachment on entrepreneurial freedom and possibly also on the freedom of communication. Here too, the model of the average consumer would not lead to such a requirement, so that in future a different consumer model, a more paternalistic one, would have to be used.
35. BEUC is also calling for a contract cancellation button. Such a button has already been introduced in German Consumer Contract Law and was now implemented in Union Law for distance contracts. The approach of the German provision itself was well received. Nevertheless, a cancellation button harbours a relevant risk of abuse, as – without proof of identity – anyone can cancel a contract with another person. For this reason, the concept of specifying a cancellation email was also proposed. Mechanisms must therefore be created to ensure that the button is not misused.
36. An interesting proposal is the introduction of a right of recourse for traders who have purchased and collected data from third-parties not controlled by them, if the data turns out to be unlawfully collected. Since data protection violations can be asserted by competitors or associations in UCPD proceedings, there might be need for such a recourse. However, this provision is very specific and foreign to the UCPD, raising questions about its necessity in the context of unlawfully collected data. It may be more appropriate to address this issue through contract law.

In addition, there may be a de facto possibility of recourse based on liability for material defects. Therefore, it is questionable whether there is a need for such a statutory provision.

37. BEUC is also calling for new rules of evidence. However, it is doubtful whether the situation described by BEUC regarding the difficulty of proving practices by consumers actually exists in general. Rather, it seems that the online environment in particular leads to documentability in a lot of cases, so that there should be no general need to make it easier for consumers to provide evidence. For the special situation of the suspicion of interface personalisation, the reversal of the burden of proof in Data Protection Law seems sufficient to uncover hidden data processing operations that take place in the background. Again, any further changes with respect to the burden of proof would need a clear identification of specific situations in which the consumer is not able to present evidence as can be considered with *scarcity* or *activity messages* patterns. Against this background, the proposed introduction of a codification of a "secondary burden of presentation and proof" is to be assessed positively. It must be examined whether such codification is necessary at European level or whether it is not already provided for by the procedural law of the Member States. However, there is much to suggest that this is a suitable means of relieving the burden on plaintiffs, and of ensuring that the facilitation of the burden of proof cannot be abused.
38. Finally, BEUC calls for further prohibitions to be included in Annex I of the UCPD. The ban on confirmshaming is particularly important for them. On the one hand, this is comprehensible because, due to its strong effect, *confirmshaming* can trigger a need for banning. However, it should be noted that particularly aggressive *confirmshaming* is already prohibited under the UCPD. In contrast to that, a far-reaching ban on *confirmshaming* that is effective below this threshold is likely to cause great legal uncertainty. It must be noted that companies have a legitimate interest in inducing and reinforcing positive connections in their communication with consumers. To a certain extent, it is legitimate for companies to follow up on a cancellation. It seems difficult to draw the line between a *fair* consumer contact as part of a normal consumer relationship management and malicious confirmation shaming below the threshold of aggressive behaviour. Against this background, the inclusion of a per se ban on *confirmshaming* seems problematic.

Overall results

39. There is therefore no need for a comprehensive recreation of the legal framework to ensure digital fairness against the backdrop of "dark patterns". In particular, there does not appear to be any need for a *revolution* in terms of abandoning the tried and tested model of the modern consumer. As it turns out, this model creates transparent and fair Consumer Law while preserving consumer sovereignty and is, as a rule, fit for the digital environment. Fundamental tightening, such as a departure from the modern consumer model, always carries the risk of a paternalistic image that cannot be reconciled with the idea of a sovereign consumer. Rather, it is advisable to carefully develop the current regulatory framework in a principle based approach and on a case-by-case basis further to create an evolution of consumer protection in the digital environment. The implementation of soft law can also be considered as a measure that can be implemented quickly. For example, the provision of guidance by the competent authorities or the introduction of certificates for compliant traders could create legal certainty and incentivise compliant behaviour.
40. Legal certainty is of particular importance for all further developments. The more unclear the rules are, the more difficult it is to enforce them. This is not helpful for consumers. At the same time, compliance costs are increased. As a first step, this is a burden for companies. But in the end, consumers will also have to pay these costs. Moreover, there is a risk of competition being distorted to the extent that particularly "aggressive" companies have an advantage over more "moderate" companies. Therefore, sensible reform steps are more likely to be seen in a case-by-case supplement to Annex I of the UCPD, for example.