The emergence of dark patterns as a legal concept in case law

Cristiana Santos (University of Utrecht)
Arianna Rossi (SnT, University of Luxembourg; Scuola Superiore Sant'Anna)

On the 23rd February 2023, the Italian Data Protection Authority (DPA) issued a decision against Ediscom S.p.A.[1] explicitly referring to "dark patterns"[2], i.e., online design choices that manipulate users' decision-making to benefit digital services. The imposed fine of 300.000 euros was due because, on some of its websites, the company employed dark patterns (hereafter DPs) to illegally entice data subjects to consent to the processing of their personal data for marketing purposes. This decision is significant as it is the first time that a DPA directly states that the use of DPs amounts to GDPR infringements, namely of the lawfulness, transparency and fairness principles (Article 5(1.a)), consent requirements (Articles 4(11), 7(2)) and data protection by design and by default (Article 25). So far, case law sanctioned[3] certain design practices without referring explicitly to DPs. This pioneer ruling sets a precedent for further regulatory decisions and case law.

Even though the term DPs is well known among the professional public, expressly mentioning DPs in decisions is a good practice for four main reasons. *First,* it can promote the adoption of a common language that is urgently needed to detect, prohibit and sanction this widespread phenomenon. *Second*, it is particularly important in light of current legislation[4] that explicitly defines DPs, e.g. Article 25 and Recital 67 of the Digital Services Act. Thus, in the future, DPs will inevitably be mentioned in legal documents such as decisions and court proceedings. *Third,* it fosters a systemic approach to DPs helping avoid fragmentation among different regulators; it connects academics, practitioners and watchdogs working on DPs; and it provides meaningful application to the knowledge, methods and tools developed by the research community. *Forth,* it may work as a deterrent for companies[5] due to the related sanctions and bad publicity. As a consequence, companies can better assess the risks and the compliance of their designs, while policymakers' can raise awareness of the scale of DP use and intensify enforcement.

---

[1] Garante per la Protezione dei Dati Personali (2023). Provvedimento prescrittivo e sanzionatorio nei confronti di Ediscom S.p.A. - 23 febbraio 2023 [9870014] https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9870014. Last accessed on 20 June 2023

[2] The term dark patterns is also referred to using different nomenclatures, e.g. deceptive design, damaging patterns, manipulative online choice architecture, or online misleading influencing techniques. However, dark patterns is now a legal term since it is mentioned in legislative documents.

[3] Deceptive Patterns Database of Legal cases, https://www.deceptive.design/cases. Last accessed on 20 June 2023

[4] Among others like Recital 70 and Article 13(4) of the Digital Markets Act, and Recital 34 and Article 6(2) of the proposed Data Act.

[5] Nowadays, dark patterns are the norm rather than the exception of online services, as it is shown by a recent study by the European Commission that demonstrates that 95% of the most used websites and applications in Europe contain at least one, European Commission (2023), Directorate-General for Justice and Consumers, Lupiáñez-Villanueva, F., Boluda, A., Bogliacino, F.et al., *Behavioural study on unfair commercial practices in the digital environment – Dark patterns and manipulative personalisation : final report*, Publications Office of the European Union, 2022, https://data.europa.eu/doi/10.2838/859030

Another important aspect of the decision is the acknowledgement of the intentional implementation of manipulative consent mechanisms: the specific design of the user interface (for example, the use of a different font for two options that should be symmetric) was not the result of a random or erroneous application. Moreover, the decision recognized that manipulation in consent interactions can impact and circumvent user's cognitive abilities, and thus subvert their autonomy and decision-making. As research shows, DPs may lead to several harms[6], such as privacy harms, cognitive burden, undue unnecessary time and attention spending, among the others.

To create the body of evidence for the decision, the DPA took screenshots of the infringing practices. To the best of our knowledge, this decision was the first that contained images in addition to textual descriptions, even if unfortunately they are published online in a low quality that makes them barely readable. Visualisations in legal literature can help demonstrate the presence of DPs and provide evidentiary examples for future decisions on similar types of interfaces.

The decision is the first to make explicit mention to the European Data Protection Board (EDPB)'s Guidelines 3/2022 on the topic[7]. Yet, it does not use any concrete DP type contained therein. Leveraging the EDPB's terms, we posit that the DPs identified in Ediscom's websites correspond to: i) ''privacy maze": users that refused consent to marketing faced an additional consent pop-up which raises unnecessary complexity in the navigation process; ii) ''lacking hierarchy'': the option to continue without consent was not easily visible but placed at the bottom of the page as a hyperlink outside the pop-up instead of a button, written in a smaller font than the rest of the text; iii) some of the websites included the option "invite a friend" wherein users were enticed to provide contact details of friends who could be potentially interested in subscribing to the service. While the EDPB does not include such a category of DP, scholarly and policy terminology coin it as ''social pyramid".[8] This lack of uniformed classification may hinder the recognition of problematic design practices in enforcement cases.

The decision refers to several other practices that could be identified as DPs.[9] This omission may be explained by the fact that consent-related DPs, especially in cookie banners, are overly represented in research and decisions, as they are more visible

[6] Johanna Gunawan, Cristiana Santos, and Irene Kamara. 2022. Redress for Dark Patterns Privacy Harms? A Case Study on Consent Interactions. In Proceedings of the 2022 Symposium on Computer Science and Law (CSLAW '22), November 1–2, 2022, Washington, DC, USA. ACM, New York, NY, USA, 14 pages. https://doi.org/10.1145/3511265.3550448.

[7] European Data Protection Board, 'Guidelines 03/2022 on Deceptive Design Patterns in Social Media Platform Interfaces: How to Recognise and Avoid Them | European Data Protection Board' (European Data Protection Board 2023) <https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-032022-deceptive-design-patterns-social-media_en> accessed 20 June 2023.

[8] OECD (2022), "Dark commercial patterns", *OECD Digital Economy Papers*, No. 336, OECD Publishing, Paris, https://doi.org/10.1787/44f5e846-en.

[9] For example, among other practices, ''dead end'': a website did not show the privacy policy before starting to collect personal data, but the link to the privacy policy was only displayed after the user was asked to consent; ''hidden in plain sight'': Ediscom asked several unnecessary questions unrelated to the service to profile users without consent, wherein the option to ignore or skip them was not clearly visible.

and easily inspectable than others. However, other design practices along the user journey of a digital service can also be problematic, even if they have been less scrutinized to date. Regardless of the narrow perspective taken in the decision, we praise the Authority for considering the user journey alongside the user interface, therefore going beyond the limited representation of DPs as static interface elements and more realistically acknowledging online processes where various DPs can be combined.

A common, shareable vocabulary must be created by the community with the purpose of detecting and describing a varied set of DPs practices to enhance legal certainty and to reliably refer to this emerging domain of practice and research. At date a plethora of siloed DPs classifications exists (often fragmented by domain, context and technology type), instead of a convergence towards a common representation of DP knowledge needed for different sectors (regulation, civil society advocates, academia, business, technologists), disciplines (law, design, computer science, economy, etc.) and goals (sanction, analyze, detect, denounce, etc.). Such vocabulary, following recent efforts[10], can raise many opportunities; it is the first step to i) enable information retrieval and traceability, ii) support the detection of DPs (through automated or manual approaches), iii) help coordinate the enforcement of different legislative instruments and reduce the risks of gaps or overlaps. For instance, the Italian DPA has already added the keyword “dark pattern” to the available tags of their online database - a useful effort that should be extended to official and unofficial searchable databases of DPA’s decisions. Meanwhile, DPAs could adopt the EDPB guidelines’ vocabulary and embed it into their decisions to have a greater impact on the prevention of manipulative practices and to tighten the relation between policy and enforcement.

[10] Colin M. Gray, Cristiana Santos, and Nataliia Bielova. 2023. Towards a Preliminary Ontology of Dark Patterns Knowledge. In Extended Abstracts of the 2023 CHI Conference on Human Factors in Computing Systems (CHI EA ’23), April 23–28, 2023, Hamburg, Germany. ACM, New York, NY, USA, 9 pages. https://doi.org/10.1145/3544549.3585676.