Alicia Maddio and Leticia Baley

Dark Patterns: the Spanish Data Protection Agency's expansive sanctioning powers

On 20 September 2023, the Spanish Data Protection Agency (using its Spanish acronym, the "**AEPD**") published an unprecedented resolution[1] (the "**Resolution**"). This is a sanctioning procedure in which, for the first time, the AEPD punishes conduct related to the inclusion of *dark patterns* on the internet, thus linking this behaviour to the breach of the duty of information established in Article 13 of Regulation (EU) 2016/679 of 27 April on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (the "**GDPR**"). The sanction amounts to €12,000 (of which €7,000 is imposed for the breach of the duty of information and €5,000 for the use of *dark patterns*).

Dark patterns are user interfaces and user experiences implemented on social media platforms, websites and apps that lead users to make unintended, unwilling and potentially harmful decisions regarding the processing of their personal data[2]. Moreover, another point to highlight in this case is the origin of the sanction, which derives from the **complaint filed by a Spanish non-profit telecommunications cooperative** under Article 82 of the GDPR.

Types of *dark patterns*

The European Data Protection Board (the "EDPB") has prepared a list of the different categories of dark patterns that may have an impact on the privacy of data subjects, and the AEPD has echoed this categorisation[3]:

- **Overloading**: this causes user fatigue, presenting the user with an excessive number of options in order to prompt them to share more information than desired (e.g., very extensive legal texts).
- **Skipping**: through the design of the interface, the user is distracted from thinking about his or her privacy (e.g., information about superfluous data is provided, omitting relevant warnings).
- **Stirring**: visual effects are used to influence users' decisions (e.g., use of bold, underlining, colours or effects for less restrictive options).

Criteria used by the AEPD to determine the sanction for the use of *dark patterns*

The AEPD considers the infringement of the **principle of fairness and transparency** (Article 5.1.a and Recital (39) of the GDPR) when identifying Overloading and Skipping *dark patterns* for the following reasons:

- The absence of a single button enabling the user to object to the processing of his data by 130 providers.
- The acceptance checkbox is ticked by default in more than half of the providers.

In addition, the AEPD uses the following circumstances to aggravate and graduate the amount of the sanction:

- The AEPD considers the scope or **purpose of the processing** carried out to be an aggravating circumstance (Article 83.2.a).

1. Resolution of the sanctioning procedure PS/00080/2023. Available at: https://www.aepd.es/documento/ps-00080-2023.pdf

2. *Guidelines* of the European Data Protection Board. Available at: https://edpb.europa.eu/system/files/2023-02/edpb_03-2022_guidelines_on_deceptive_design_patterns_in_social_media_platform_interfaces_v2_en_0.pdf

3. For more information, on 19 May 2022, the AEPD published the entry *Dark patterns* on its public blog: *Manipulation in Internet services*, available at: https://www.aepd.es/prensa-y-comunicacion/blog/dark-patterns-manipulacion-en-los-servicios-de-internet)

- **Hindering**: this makes it difficult for the user to perform actions straightforwardly (e.g., adding unnecessary steps).
- **Fickle**: this means that the interface is designed in an unstable and inconsistent way, hindering the understanding of the data processing to be performed and making it difficult to make decisions (e.g., clicking on an option automatically changes the language).
- **Left in the dark**: information or privacy settings options are hidden or presented in an unclear way using erratic language, or contradictory or ambiguous information.

- In addition, the AEPD imposes a second aggravating circumstance because it considers that the **activity** carried out by the company - aimed at putting lawyers in contact with potential clients - **is closely linked to the processing of personal data** (Article 76.2.b) of Organic Law 3/2018, of 5 December, on the Protection of Personal Data and the Guarantee of Digital Rights).

Why is this resolution relevant?

1. Although the AEPD has introduced this type of conduct in its Guide to Data Protection by Default[4] , this is the first case in which it has sanctioned a data controller for the use of *dark patterns*.
2. Until now, this conduct was sanctioned on the basis of some other breach of consumer or user regulations, or even by the AEPD, although without using this classification, which is more typical of other sectors.
3. From now on, there could be an overlapping of sanctioning procedures, firstly in consumer and user matters, and secondly, for the breach of data protection regulations.
4. The trend at European level seems to suggest that the authorities in other Member States have also turned their attention to this type of conduct[5].

Main online services vulnerable to such breaches

Social networks

Users share a high volume of personal information and are exposed to many opt-in processes for the processing of their data.

Video games

Users may interact with publishers through interactions that may have an impact on their rights or involve their acceptance of specific economic conditions (e.g., through the purchase of loot boxes).

Websites that target consumers

On websites where users can create user accounts, there are different stages where *dark patterns* can be introduced (first visit, banner and cookie policy, privacy policy, and different consents, among others).

Available at: https://www.aepd.es/documento/guia-proteccion-datos-por-defecto.pdf

5. The Italian authority (*Garante per la Protezione dei Dati Personali)* has also, for the first time, sanctioned a company for the use of *dark patterns*, imposing a fine of €300,000. Resolution available at: https://garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9870014#

How to avoid committing this type of breach?

1. It is essential to consider, at all times, the **principles of fairness and transparency** contained in the GDPR, as well as consumer and user regulations.
2. Guarantee **data protection by design and by default** (e.g., when introducing the option to make purchases within a video game, ensure that users can easily reject this option from the production and design phase of the application).
3. Be fully aware of the EDPB's recommendations and integrate mechanisms that allow users to control the destination of their personal data.

Some of the best practices recommended by the EDPB to prevent sanctions are

Shortcuts

Introducing visible links within the interface that take the user directly to the privacy settings so that they can exercise their rights and adjust their preferences.

Bulk options

Putting options that have the same processing purpose together, so that users can change them more easily, in a single action.

Use of coherent wording

Pay particular attention to ensure that definitions and terms relating to data protection are the same in all parts of the interface, in order to make it easier for the user to understand.

Does this resolution open the door to massive claims for damages for the use of dark patterns?

The recognition of this sanction by the AEPD involves a risk for data controllers for the following reasons:

General issues

- The complaint that led to this sanctioning Resolution was filed by a Spanish **non-profit telecommunications cooperative** providing user advocacy services.
- This is evidence that a number of different stakeholders have already taken steps to organise themselves and bring complaints on behalf of affected data subjects.
- The GDPR opens the door to massive claims for **compensation for damage as a consequence of a breach of the GDPR**. Specifically, the grounds for standing to bring such actions are provided for in Article 82 of the GDPR, in conjunction with recital (146).

Particular issues

- By their very nature, the use of *dark patterns* may impact a **large number of users** and not just a limited number, so the risk of a significant impact is high.
- *Dark patterns* may lead the user to perform **actions that are easily quantifiable from the perspective of claims for damages** (e.g., consumer subscription to paid services or sharing more information than desired).
- The fact that the AEPD has for the first time identified this conduct as liable to sanctions may lead to a **stricter definition of these concepts, which in turn will involve automated identification of irregularities** by data subjects.

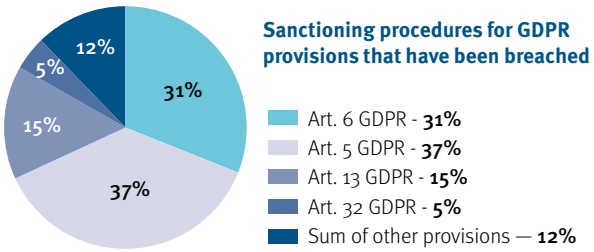
- On 23 May 2023, the **Court of Justice of the European Union**[6] resolved the interpretative doubts that could exist regarding the practical application of Article 82 of the GDPR, establishing that it will apply when, cumulatively:

  i) There has been a breach of the GDPR.

  ii) It is possible to establish the actual existence of damage.

  iii) There is a causal link between the damage and the breach.

- The AEPD links the inclusion of *dark patterns* (a breach of Article 5.1.a of the GDPR) with the breach of the duty to provide information (Article 13 of the GDPR), as these are the provisions with the greatest impact in terms of sanctions imposed by the AEPD[7]:



- The use of *dark patterns* can be seen in a **variety of different situations**, putting a lot of pressure on data controllers to ensure an adequate level of compliance at all levels:

  – When first **developing software or a website**, it is necessary to ensure that it is, by default, compliant with data protection and consumer and user regulations, and does not impose unnecessary burdens on users when performing actions.

  – Subsequently, when **designing and configuring the graphical interface**, it is necessary to provide a simple and transparent decision-making process for users.

  – In addition, the legal texts should use clear and direct language, favouring compliance with the duty to provide information and avoiding the concealment of relevant details on data processing.

6. Judgment of the CJEU available here: https://curia.europa.eu/juris/document/document.jsf;jsessionid=2EB8A1175E9096F7BB3B08C-C86255693?text=&docid=273284&pageIndex=0&doclang=es&mode=req&dir=&occ=first&part=1&cid=2541832

7. Proprietary graph, based on the information published on the AEPD website (Resolutions section) and filtering by type of procedure (Sanctioning procedure) and Law (GDPR) since 2018.

CONTACTS

Raúl Rubio
Partner, Intellectual Property and Technology
rrubio@perezllorca.com
T. +34 91 353 45 59

Andy Ramos
Partner, Intellectual Property and Technology
aramos@perezllorca.com
T. +34 91 423 20 72