Addictive patterns in the processing of personal data

Implications for data protection

July 2024

CONTENTS

I. INTRODUCTION

Entities that use the Internet to provide platforms, applications and services process personal data. Such personal data processing should generally be lawfully based on the performance of a contract laid down in the terms of service. Personal data processing could also be lawfully established with other legal bases, mainly the data subject’s consent or legitimate interests pursued by the provider (for security purposes, for example).

According to the European Data Protection Board (EDPB): “While some of these services are funded by user payments, others are provided without monetary payment by the consumer, instead financed by the sale of online advertising services allowing for targeting of data subjects. Tracking of user behaviour for the purposes of such advertising is often carried out in ways the user is often not aware of, and it may not be immediately obvious from the nature of the service provided, which makes it almost impossible in practice for the data subject to exercise an informed choice over the use of their data”[1].

With this model, providers' profits depend largely on the amount of time the user spends using their products, the user's involvement or commitment, and the amount of data collected from the data subjects themselves and their network of personal contacts. Improving such factors makes improving the return on investment possible, by enhancing user segmentation for marketing and ads, increasing user loyalty, or finding new ways to monetise personal data.

Therefore, some Internet providers try to keep users on the platform, application, or service for as long as possible and influence or manipulate their behaviour by including additional operations to personal data processing based on deceptive and addictive design patterns.

Deceptive patterns are considered as interfaces and user experiences implemented on social media platforms that lead users to make unintended, unwilling and potentially harmful decisions regarding processing their personal data[2]. Addictive patterns will be defined in this document as design features, attributes or practices that determine a particular way of using digital platforms, applications and services intended to make users spend much more time using them or with a greater degree of commitment than what is expected, convenient or healthy for them. Both characteristics of a design pattern, its deceptive and addictive nature, are closely related, although they are not the same.

Adding such operations implementing addictive patterns to personal data processing has implications for several data protection aspects, like the lawfulness of the processing (in particular over the consent conditions or the prohibition to processing special categories of personal data), fairness and transparency, purpose limitation, data minimization, data protection by design and by default, and accountability.

Regarding the principle of accountability, the use of such patterns raises concerns about disregarding of the risk to the users’ rights and freedoms that implies the addition of such operations to personal data processing. Their impact may be particularly severe on the right to physical and mental integrity of children and younger users, potentially affecting their way of making decisions and relating to society, or their mental balance.

[1] Paragraph 4 in the EDPB Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects. Version 2.0 8 October 2019. https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-22019-processing-personal-data-under-article-61b_en

[2] EDPB Guidelines 03/2022 on Deceptive design patterns in social media platform interfaces: how to recognise and avoid them. Version 2.0. Adopted on 14 February 2023 https://www.edpb.europa.eu/system/files/2023-02/edpb_03-2022_guidelines_on_deceptive_design_patterns_in_social_media_platform_interfaces_v2_en_0.pdf

A. REGULATION REGARDING DECEPTIVE AND ADDICTIVE PATTERNS

The European Union (EU) is increasingly recognising the need to address deceptive and addictive design patterns in online services.

The EDPB addressed the issues about deceptive patterns in the "Guidelines 03/2022 on deceptive design patterns in social media platform interfaces: how to recognise and avoid them"[1]. These guidelines are focused only on deceptive patterns in social media, and the document addresses their implications for fairness, transparency, accountability, data protection by design and GDPR compliance. Moreover, it was stated that data protection authorities are responsible for sanctioning the use of deceptive design patterns if these breach GDPR requirements.

The European Parliament adopted a resolution in December 2023 explicitly addressing the addictive design of online services and consumer protection in the EU single market[3]. The resolution calls for banning addictive practices such as endless scrolling or automatic play that encourage prolonged engagement, moving from attention economy to ethical design, introducing a digital right to "not be disturbed", empowering users to control their online experiences and ensuring that all online platforms, applications and services are safe for children to use and introducing new consumer legislation specifically targeting addictive practices.

Beyond the EU, various countries and international bodies have also recognised the impact of addictive practices online. For instance, the United Nations has highlighted the need to address digital addiction and protect children's rights in the digital environment[4]. However, specific regulations vary by country. Some have implemented guidelines or laws related to the addictive features of technology, while others are still exploring practical approaches. For example, the Stop Addictive Feeds Exploitation (SAFE) for Kids Act[5], passed by the New York's Legislature in June 2024, will prohibit social media platforms from serving content to users under the age of 18 based on recommendation algorithms under certain circumstances. Instead, these platforms will have to provide reverse-chronological feeds[6] for young users.

As technology evolves, policymakers worldwide try to find the right balance between innovation, user experience, and user health. The EU is actively discussing additional measures to regulate the addictive design and protect users as consumers, specifically those more vulnerable to these patterns[7]. However, the concept of vulnerability must not be restricted to traditionally protected groups. Still, it must include all consumers because addictive design patterns have become so sophisticated that they are capable of finding and exploiting the weaknesses or vulnerabilities of any average individual.

The Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act), addresses various aspects of digital services and their impact on users.

[3] European Parliament resolution of 12 December 2023 on addictive design of online services and consumer protection in the EU single market (2023/2043(INI)) https://www.europarl.europa.eu/doceo/document/TA-9-2023-0459_EN.html

[4] Child and Youth Safety Online https://www.un.org/en/global-issues/child-and-youth-safety-online

[5] Senate Bill S7694A, 2023-2024 Legislative Session, Establishes the Stop Addictive Feeds Exploitation (SAFE) for Kids Act prohibiting the provision of addictive feeds to minors https://www.nysenate.gov/legislation/bills/2023/S7694/amendment/A

[6] A feed is a stream of content that the user can scroll through. It can be personalised by a recommender or purely chronological, showing new content. In this second case, new content can be displayed at the beginning of the feed (reverse order) or at the end, forcing the user to scroll through it continuously to access the latest publications.

[7] There are already sanctions imposed by consumer authorities, such as this recent one from the Netherlands authority: https://www.acm.nl/en/publications/acm-imposes-fine-epic-unfair-commercial-practices-aimed-children-fortnite-game

This act recognises the need to regulate certain practices that can lead to addictive[8] behaviours or harm to users, and the use of deceptive designs[9].

The proposed Artificial Intelligence Regulation can also play a role in shaping the digital landscape in relation to addictive patterns when implemented through artificial intelligence systems and models. This type of system can be the basis of some addictive patterns and, therefore, would be subject to the prohibitions established in Article 5, as long as they are related to subliminal, manipulative, deceptive techniques or that exploit vulnerabilities of individuals or groups of people, mainly due to their age, with the aim of affecting a person's decisions or behaviour and causing them harm.

B. THE AEPD PROJECT

The EDPB has analysed deceptive patterns from the GDPR perspective for specific use cases. The AEPD, within the framework of its obligations to carry out technological prospecting studies[10], has conducted internal activities around a research project based on a systematic review of the existing scientific evidence about addictive patterns (following the PRISMA-ScR method[11]), which means addressing new use cases. Therefore, the EDPB guidelines can be augmented, and a unified understanding of such patterns is allowed, since some of them could have deceptive and addictive characteristics simultaneously. Sections II and III of this document summarise this project's results.

The performed research enables an exhaustive analysis of the data protection implications of including deceptive and addictive patterns in personal data processing. Therefore, this document draws conclusions at different levels about the implications of these patterns on data protection and the rights and freedoms of individuals; these are introduced in section IV.

[8] Recital 81: "Such risks may arise, for example, about the design of online interfaces which intentionally or unintentionally exploit the weaknesses and inexperience of minors or which may cause addictive behaviour" and Recital 83: "Such risks may also stem from coordinated disinformation campaigns related to public health, or from online interface design that may stimulate behavioural addictions of recipients of the service". In addition, articles 27 and 38 imply obligations for recommender systems, usually closely related to addictive behaviours.

[9] Recital 67 and Article 25: "Providers of online platforms shall not design, organise or operate their online interfaces in a way that deceives or manipulates the recipients of their service or in a way that otherwise materially distorts or impairs the ability of the recipients of their service to make free and informed decisions".

[10] Article 31(c) of Royal Decree 389/2021, of June 1, which approves the Statute of the Spanish Data Protection Agency (AEPD).

[11] Tricco, A. C. et al. (2018). PRISMA extension for scoping reviews (PRISMA-ScR): checklist and explanation. Annals of internal medicine, 169(7), 467-473.

II. ADDICTIVE PATTERNS: DEFINITION AND CONTEXT

The development of addictive patterns starts with the notion of persuasive technology[12] promoted in the 90s. The idea was to take advantage of specific aspects of technological developments to positively influence users, specifically in their living attitudes and behaviour: health, sleep, study, etc. The definition given by Fogg back then was "interactive computing systems designed to change people's attitudes and behaviours, without using coercion or deception".

Over the years, persuasive technology has become ubiquitous, being integrated into video games, social networks, and mobile apps. This evolution has been motivated mainly by the need of technology companies to prolong users' time on their platforms and services (indirect monetisation through digital marketing and advertising) and to engage them with a higher level of commitment (direct monetisation through the purchase of different goods and services). Therefore, the definition of persuasive technology has changed. For example, "any information system that proactively affects human behaviour, in or against the interests of its users"[13].

Previous work has identified different features related to persuasive technology[14], such as objectives, feedback, reminders, alerts, triggers, rewards, points, credits, tracking, monitoring, or social support, sharing and comparison. Most of these features need to be personalised to work, therefore the provider must capture and process users' personal data. For this reason, among others, such as scalability or cost reduction, all these features have in common their autonomy and high degree of automation. The advances of paradigms such as machine learning or artificial intelligence have greatly favoured both aspects.

Persuasive design, when applied to platforms, applications and services, makes them addictive[15]. A reduced set of persuasive features devoted to manipulating users' attention is being regularly included in many platforms, applications and services as a model or guide, becoming patterns. Addictive patterns, to be accurate.

In this document we define an addictive pattern as:

A design feature, attribute or practice that determine a particular way of using digital platforms, applications and services intended to make users spend much more time using them or with a greater degree of commitment than what is expected, convenient or healthy for them.

Addictive patterns not only result in a longer time of use of the platforms, applications or services. They may cause more significant commitment, reaching dependence, implying that users prefer their use instead of carrying out other activities, even essential ones, such as eating, sleeping, or interacting with others. Or encouraging them, for example, to make a disproportionate financial expense or to share sensitive information. Problems in establishing personal relationships, fragmentation of attention, alteration in mental decision-making mechanisms or a negative perception of life satisfaction may arise. These effects are especially significant in childhood and adolescence.

[12] Fogg, B. J. (1998). Persuasive computers: perspectives and research directions. In *Proceedings of the SIGCHI conference on Human factors in computing systems* (pp. 225-232).

[13] Kampik, T., Nieves, J. C., & Lindgren, H. (2018). Coercion and deception in persuasive technologies. In *Proceedings of the 20th International Trust Workshop (co-located with AAMAS/IJCAI/ECAI/ICML 2018)* (pp. 38-49).

[14] Orji, R., & Moffatt, K. (2018). Persuasive technology for health and wellness: State-of-the-art and emerging trends. Health informatics journal, 24(1), 66-91.

[15] Chen, X., Hedman, A., Distler, V., & Koenig, V. (2023). Do persuasive designs make smartphones more addictive? A mixed-methods study on Chinese university students. Computers in Human Behavior Reports, 10, 100299.

In almost all scenarios, users cannot turn off these features, even when they perceive their negative influence or impacts.

A. Deceptive and addictive patterns

There is a certain degree of intersection between the concept of deceptive pattern (or dark pattern) and that of addictive pattern that should be clarified at this time. Consider, for example, three definitions that may be of interest to provide some initial context.

The first is the one provided by the EDPB in the aforementioned guidelines on deceptive design patterns in social media: “Deceptive design patterns are considered as interfaces and user journeys implemented on social media platforms that attempt to influence users into making unintended, unwilling and potentially harmful decisions, often toward a decision that is against the users’ best interests and in favour of the social media platforms interests, regarding the processing of their personal data. Deceptive design patterns aim to influence users’ behaviour and can hinder their ability to effectively protect their personal data and make conscious choices”.

The second is the OECD definition for dark pattern. Dark pattern is an umbrella term referring to a wide variety of practices commonly found in online user interfaces that lead consumers to make choices that often are not in their best interests[16]. The definition given by the OECD is “Dark commercial patterns are business practices employing elements of digital choice architecture, in particular in online user interfaces, that subvert or impair consumer autonomy, decision-making or choice. They often deceive, coerce or manipulate consumers and are likely to cause direct or indirect consumer detriment in various ways, though it may be difficult or impossible to measure such detriment in many instances”.

And the third is the definition provided by the Digital Services Act in its preamble (recital 67): “Dark patterns on online interfaces of online platforms are practices that materially distort or impair, either on purpose or in effect, the ability of recipients of the service to make autonomous and informed choices or decisions. Those practices can be used to persuade the recipients of the service to engage in unwanted behaviours or into undesired decisions which have negative consequences for them”.

Previous research has also provided different definitions[17], all of them similar to these three and focused on the same aspects: deception, manipulation, influence, making decisions against one's own interests, potential harm or negative consequences, lack of choice and information, etc.

Therefore, we conclude that all addictive patterns can be considered deceptive patterns, but not all deceptive patterns are addictive (see Figure 1). For example, there are a significant number of deceptive patterns focused on making it hard to cancel an account or service, adding charges to a transaction at its final stage, etc., without the capability to cause addiction.

[16] OECD Digital Economy Papers, n336 (2022). Dark commercial patterns. https://one.oecd.org/document/DSTI/CP(2021)12/FINAL/en/pdf

[17] Cara, C. (2019). Dark patterns in the media: A systematic review. *Network Intelligence Studies*, 7(14), 105-113.

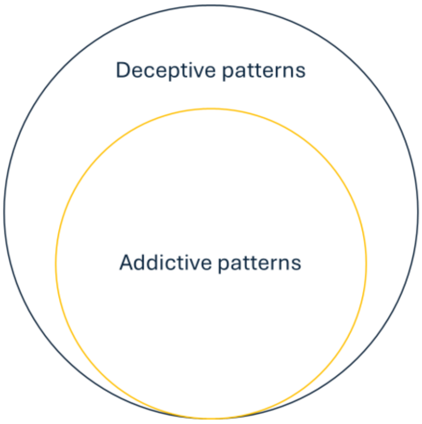


Figure 1. Considered relationship between deceptive patterns and addictive patterns

B. ADDRESSABILITY

Many social media platforms provide segmentation and targeting services as part of their business model. These services enable individuals or organizations ("targeters") to convey specific messages to social media users to promote political or commercial interests. The critical aspect of segmentation and targeting is the perceived alignment between the targeted individual or group and the conveyed message. The underlying assumption is that the better the alignment, the higher the reception rate (conversion), leading to a more effective targeting campaign (return on investment)[18].

In the case of addictive patterns, the "targeters" are the providers of digital platforms, applications and services themselves, not a third party. And their strategy does not seek to deliver a specific political or commercial message to a particular person or group, but rather to ensure that the user remains connected for longer or with a greater degree of commitment. In this document we will use the word addressability to refer to these ultra personalised strategies carried out for addictive rather than political or commercial purposes.

Addressability, as targeting, makes users' directly accessible to appealing or influence. In this case, through their weaknesses or vulnerabilities, as individuals or as members of a dynamic and reduced group. But the techniques used, and the processing of personal data involved, are very similar to those of political or commercial targeting much more analysed so far. The EDPB, in its document "Guidelines 8/2020 on the targeting of social media users" provides guidelines that are useful in the context of the addressability carried out by operations that implement addictive patterns.

C. ADDICTIVE PATTERNS OPERATING MODEL

The framework shown in Figure 2 is based on already validated models[19] and includes the different elements concerning addictive patterns and their context. Platforms, applications, and services are designed to maximize their benefits considering their specific business

[18] EDPB Guidelines 8/2020 on the targeting of social media users Version 2.0 Adopted on 13 April 2021. https://www.edpb.europa.eu/system/files/2021-04/edpb_guidelines_082020_on_the_targeting_of_social_media_users_en.pdf

[19] Montag, C., Yang, H., & Elhai, J. D. (2021). On the psychology of TikTok use: A first glimpse from empirical findings. *Frontiers in public health*, *9*, 641673.

model. The Stigler Committee[20] concluded in 2019 that the business model of major online platforms is based on addictive user interface designs to maintain users' attention.

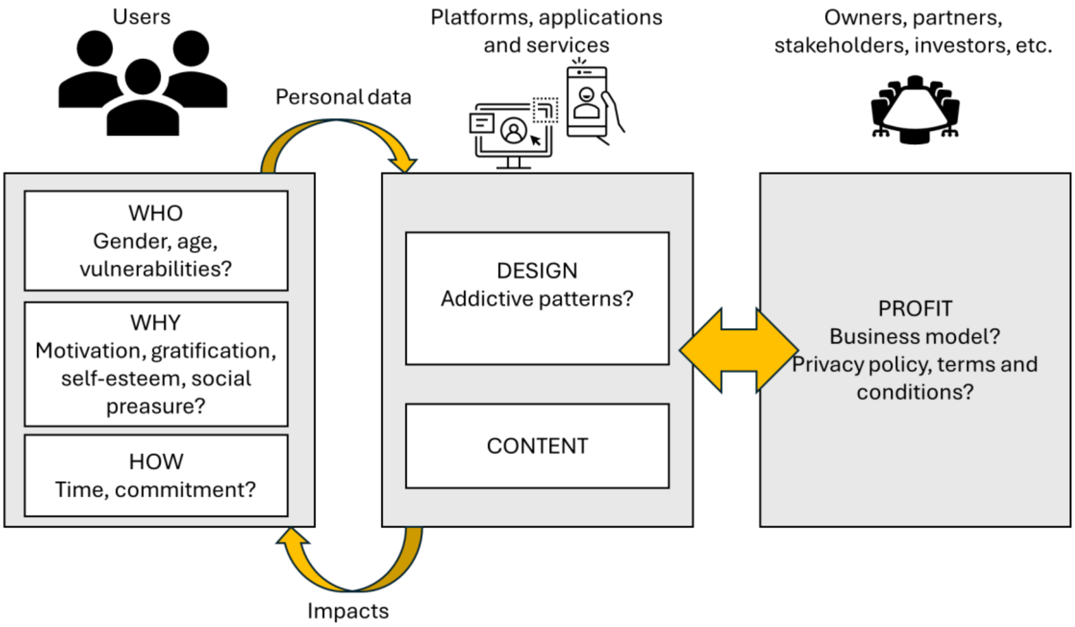

Users
Platforms, applications and services
Owners, partners, stakeholders, investors, etc.
Personal data
WHO
Gender, age, vulnerabilities?
WHY
Motivation, gratification, self-esteem, social preasure?
HOW
Time, commitment?
DESIGN
Addictive patterns?
CONTENT
PROFIT
Business model?
Privacy policy, terms and conditions?
Impacts

Figure 2. Addictive patterns context

These addictive patterns may need to be fed with users' personal data and may impact their health and well-being. What specific data could be gathered and what these impacts could be is dependent on who these users are, why they use the platforms, applications, and services, and how they use them. Because users with different mental, social, technological and behavioural backgrounds may react differently to the same design feature[21].

Platforms, applications and services providers are incentivised to design their products in a way that perform well in terms of profit and metrics relevant to their business model. According to these metrics, and given the current market pressure, when employing addictive patterns, they may obtain better results[22].

All these providers monetise users' engagement (time and commitment), mainly through advertising. Therefore, the metrics relevant to their business model are the metrics standardized within the digital advertising market[23]. These metrics identify the measurements that providers must perform to certify when an ad has been delivered to a user and it should be billed. And allows providers to explore design and content features that optimize these metrics values.

[20] Independent and non-partisan Committee composed of more than thirty academics, policymakers, and experts at the USA that spent over a year studying how digital platforms such as Google and Facebook impact economy and antitrust laws; data protection; the political system; and the news media industry: https://www.chicagobooth.edu/research/stigler/news-and-media/committee-on-digital-platforms-final-report

[21] Sindermann, C., Montag, C., & Elhai, J. D. (2022). The Design of Social Media Platforms—Initial Evidence on Relations Between Personality, Fear of Missing Out, Design Element-Driven Increased Social Media Use, and Problematic Social Media Use.

[22] Narayanan, A., Mathur, A., Chetty, M., & Kshirsagar, M. (2020). Dark Patterns: Past, Present, and Future: The evolution of tricky user interfaces. Queue, 18(2), 67-92.

[23] Interactive Advertising Bureau (IAB) https://www.iab.com/

In short, data represent two different types of value in this context:

1. They allow providers to quantify performance through standardised metrics and demand payment from advertisers: audience reach measurement (unique users, visits, time spent).
2. They allow providers to optimise performance knowing exactly what to offer each user so that they stay online for as long as possible with the maximum possible commitment. In this case there are not standardised metrics. Providers may know or infer using different methods the following data:
   - User data: Account name, email address, persistent identifiers or pseudonyms, language, age/date of birth, gender, etc.
   - Connection fingerprint: Device features (processor, memory and graphics card information, screen parameters, audio parameters, operating system version, time zone), browser features (version, list of plug-ins, language list, user-agent header, ad-block information, web storage mechanisms, screen resolution available), IP address, geolocation, etc.
   - User behaviour: How does the user interact with the platform, application or service? What is the user usual journey? What functionalities does the user consume more often? How?
   - User habits and preferences: How much time is the user connected on average? At what time? What content does the user prefer? At what point in a video does the user tend to share, like or dismiss it? Does the user tend to interact with other users? With whom? And with ads?

Providers profits are highly dependent on the number of users, the amount of time each user spends connected and their degree of commitment, and the amount of data a user provides, directly or indirectly. Recent research coins the term “data-attention imperative”[24]. This imperative occurs in both directions. On one hand, providers accumulate and use data to design more engaging and addictive experiences for users. On the other hand, they are driven to increase engagement and attentional supply to produce data and generate profits. The role of data, in this context, is to transform users’ attention and behaviour into a monetizable good within a cyclical process: the data that is gathered during users’ interaction with the platforms can be marketed directly, for example, to advertisers. But they can also be used to exploit users' vulnerabilities (trough addressability), gain their attention and commitment, and make them spend more time online.

The available research points out persistent and widespread psychological weaknesses or vulnerabilities and cognitive biases which are usually exploited by addictive patterns to achieve this goal such as (this is not an exhaustive list):

- **Affect heuristic:** Content eliciting positive emotions significantly influences user’s decisions.
- **Anchoring:** Users rely too heavily on the first piece of information offered (the “anchor”) when making decisions.
- **Automation bias:** Users tend to rely excessively on automated or algorithmic systems.
- **Default effect:** Users are unlikely to change default configurations and settings to deselect a pre-selected checkbox, etc.

[24] Bietti, E. (2024). The Data-Attention Imperative. Available at SSRN 4729500 http://dx.doi.org/10.2139/ssrn.4729500

- **Effort justification:** Users attribute more significant value to an outcome if they had to put effort into achieving it.
- **Framing effect:** Users draw different conclusions from the same information depending on how that information is presented.
- **Illusion of control:** Users tend to overestimate their degree of influence over external events.
- **Instant gratification:** Users tend to sacrifice future gain for immediate pleasure or gain.
- **Investment:** If the user is committed to the task, they want to see the result or the end.
- **Loss aversion:** Users feel the pain of loss twice as intensively as the equivalent pleasure of gain.
- **Ostrich effect:** Users tend to ignore obvious negative situations.
- **Pro-innovation bias:** Users tend to show excessive optimism towards new platforms, applications and services while often failing to identify their limitations and weaknesses.
- **Self-assessment issues:** Users may overestimate their own ability (for example, the capability of detecting deceptive or manipulative designs), underestimate the influence of visceral drives on their behaviours, believe that they are in complete control and autonomous, etc.
- **Social norms:** Users feel constrained or guided by unwritten rules and social standards understood by the rest of the group users.
- **Status quo:** Users often prefer an option that causes no change, the “traditional” one.

III. ADDICTIVE PATTERNS CLASSIFICATION

In this section we propose a classification of addictive patterns following the most recent three-level (high, meso, low) ontology available in the literature to create a shared language about this topic[25]. In this way, high-level patterns correspond to the most abstracted knowledge, referring to general strategies in a context-agnostic and application-agnostic way. Four of them have been identified: Forced Action, Social Engineering, Interface Interference and Persistence. Meso-level patterns describe more specific approaches to follow these strategies, exploiting specific users' psychological weaknesses or vulnerabilities, but they are still context and application-agnostic. Finally, low-level patterns correspond to specific execution of the different approaches, they are often context or application specific. And they may be detected through algorithmic, manual, or other technical methods. This classification is summarised, along with other aspects, in Table 1 of section IV of this document.

All these identified patterns may use or require personal data as input, collect or generate new personal data, or influence user behaviour within the framework of personal data processing.

Our classification considers patterns already identified and analysed in previous research[26],[27],[28],[29],[30],[31],[32],[33],[34],[35] focusing on their addictive trend given the available evidence (analysed conducting a systematic review following the PRISMA-ScR method). Therefore, on those demonstrated to manipulate users to spend much more time using platforms, applications and services, or with a greater degree of commitment than expected. Different patterns have been merged or unfolded to avoid redundancies or gaps; work has also been done to unify the nomenclature.

The provided classification is as comprehensive as possible, but new patterns may be found (especially at the third level, as they are highly context and platform, application or service dependent) or created. And identified patterns will evolve in the future. That is, it is expected to be a live list that must be completed over time.

It is also worth noting that some patterns often appear together or that the same pattern could appear in two different high-level categories. We have tried to make them as independent from each other as possible and always classify them into a main category with which they are most related.

[25] Gray, C. M., Santos, C., & Bielova, N. (2023, April). Towards a Preliminary Ontology of Dark Patterns Knowledge. In Extended Abstracts of the 2023 CHI Conference on Human Factors in Computing Systems (pp. 1-9).

[26] Zagal, J. P., Björk, S., & Lewis, C. (2013). Dark patterns in the design of games. In Foundations of Digital Games 2013.

[27] Gray, C. M., Kou, Y., Battles, B., Hoggatt, J., & Toombs, A. L. (2018, April). The dark (patterns) side of UX design. In Proceedings of the 2018 CHI conference on human factors in computing systems (pp. 1-14).

[28] Montag, C., Lachmann, B., Herrlich, M., & Zweig, K. (2019). Addictive features of social media/messenger platforms and freemium games against the background of psychological and economic theories. International journal of environmental research and public health, 16(14), 2612.

[29] Mathur, A., Acar, G., Friedman, M. J., Lucherini, E., Mayer, J., Chetty, M., & Narayanan, A. (2019). Dark patterns at scale: Findings from a crawl of 11K shopping websites. Proceedings of the ACM on Human-Computer Interaction, 3 (CSCW), 1-32.

[30] Gray, C. M., Chivukula, S. S., & Lee, A. (2020, July). What Kind of Work Do" Asshole Designers" Create? Describing Properties of Ethical Concern on Reddit. In Proceedings of the 2020 ACM designing interactive systems conference (pp. 61-73).

[31] Gray, C. M., Santos, C., & Bielova, N. (2023, April). Towards a Preliminary Ontology of Dark Patterns Knowledge. In Extended Abstracts of the 2023 CHI Conference on Human Factors in Computing Systems (pp. 1-9).

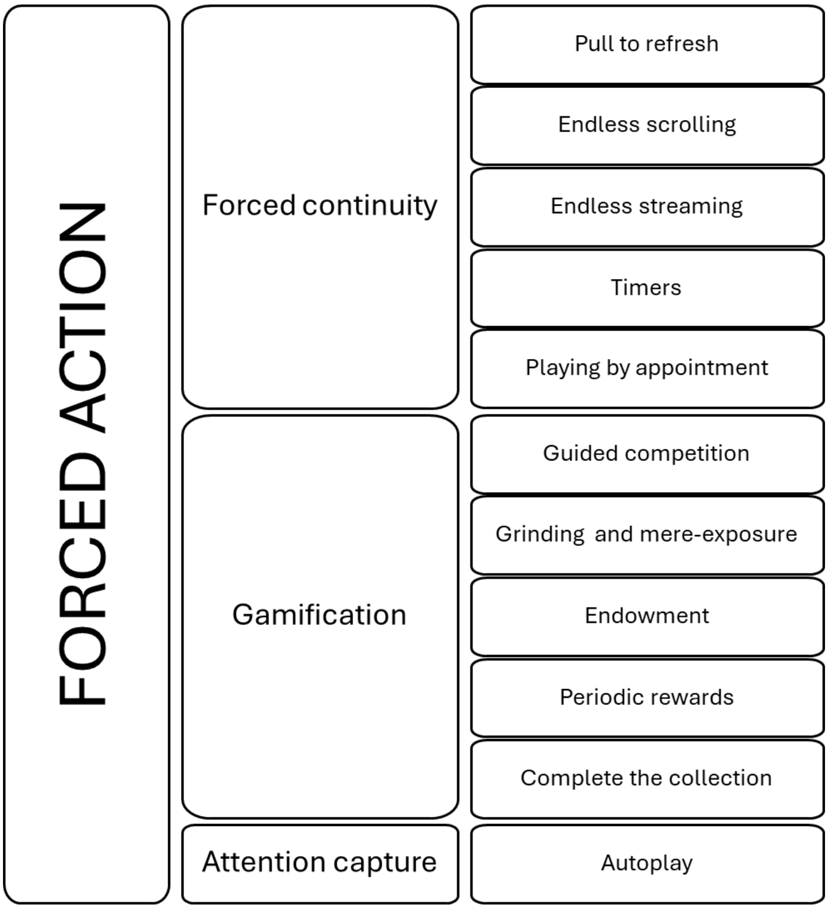
[32] Mildner, T., Savino, G. L., Doyle, P. R., Cowan, B. R., & Malaka, R. (2023, April). About Engaging and Governing Strategies: A Thematic Analysis of Dark Patterns in Social Networking Services. In Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems (pp. 1-15).

[33] Flayelle, M., Brevers, D., King, D. L., Maurage, P., Perales, J. C., & Billieux, J. (2023). A taxonomy of technology design features that promote potentially addictive online behaviours. Nature Reviews Psychology, 2(3), 136-150.

[34] OECD Digital Economy Papers, n336 (2022). Dark commercial patterns. https://www.oecd.org/digital/dark-commercial-patterns-44f5e846-en.htm

[35] EDPB Guidelines 03/2022 on Deceptive design patterns in social media platform interfaces: how to recognise and avoid them. Version 2.0 adopted on 14 February 2023. https://www.edpb.europa.eu/system/files/2023-02/edpb_03-2022_guidelines_on_deceptive_design_patterns_in_social_media_platform_interfaces_v2_en_0.pdf

A. FORCED ACTION



FORCED ACTION	Forced continuity	Pull to refresh
		Endless scrolling
		Endless streaming
		Timers
		Playing by appointment
	Gamification	Guided competition
		Grinding and mere-exposure
		Endowment
		Periodic rewards
		Complete the collection
	Attention capture	Autoplay

This high-level category consists of offering users something they want requiring them to do something in return or tricking them to do it in a way that may cause them a detriment, whether they are aware or not.

Forced continuity

This approach is directly related to time, it includes features that make users spend more time connected than expected or do so at times that are not the best for them. Although there is a coercion or pressure, users should perceive their session prolongation as something natural and smooth, freely decided.

- **Pull to refresh:** This pattern is based on a gesture consisting of touching the screen with a finger, and then releasing it, as a signal to the application to refresh the contents of the screen, in real time. It is usually combined with Algorithmic recommendations to offer the user personalised content after each refresh, more likely to hold their attention.
- **Endless scrolling:** Users can scroll seamlessly through content rather than clicking through different pages. It is usually combined with Algorithmic recommendations to offer the user personalised content more likely to engage them.
- **Endless streaming:** When a song or a video finish, the next video begins without user’s interaction (a similar content, the next episode, etc.). It is usually combined with Algorithmic recommendations to offer the user personalised content more likely to engage them.

- **Timers:** This pattern is based on making users arbitrarily wait for something. For example, some online games make users wait an arbitrary amount of time before a task is completed. Social networks often reward consistent engagement too, users are encouraged to log in a specific arbitrary amount of time to earn rewards or complete challenges.

Example:

Imagine a fantasy game. The gamer wants to forge a legendary sword, and the game allows the gamer to craft it, but this task will take 4 hours to complete. The gamer can't speed up the process; just wait.

During these 4 hours, the gamer keeps connected to the game. It may be running in the background, but the gamer will likely make periodic checks on the progress of the process.

The gamer will need 1 day to update the castle. To train troops, 2 days. And so on for other valuable resources.

This is effective because it guarantees retention; once the timer has finished, gamers will interact with the game to claim the results (the sword, the new castle, etc.). And in some cases, this pattern enables monetization. For example, the gamer can bypass the timer using in-game currency (gems, coins). In this case, the pattern encourages commitment.

If timers are too long, too frequent or related to resources perceived as "low value" by gamers, they can feel frustrated or lose interest. Game designers must strike a balance between anticipation and annoyance. They profile gamers depending on their habits (gaming session length, game schedule, game frequency, game preferences, spending history, etc.) to optimize all these features.

- **Playing by appointment:** Users don't decide when to connect or to play, other users or the provider decide for them. If a user does not connect or play according to this "appointment" may be penalized. This pattern, as its name suggests, is usually found in online videogames. But Adult content platforms can make users wait for a new content, social networks to a specific post from a prominent profile or to the announcement of a specific promotion. Scheduled content drops, live-streams or special events have similar effects than appointments to play: flash-sales, influencers live-streams, etc.

Example:

Imagine a brand running a 1-hour flash sale on a social network where users can access exclusive products and discounts.

Users have had to interact with the social network that hosts it enough to find out the specific time and connect during that time to have access to the benefits promised in advance.

If flash-sales are not disseminated enough among their target audience and they do not find out that they occur, or they find out, but the schedule does not suit them at all or does not motivate them enough, the performance metrics of this pattern will be poor.

Campaign designers must find the way to guarantee enough engagement, determining when and to whom certain contents are shown. They profile the social network users depending on their habits and preferences to optimize all these features concerning dissemination (who receives the information, how and when) and the campaign itself (how long does it last and at what time, how often is it done, what products or discounts are offered and how are they offered).

Gamification

This approach is directly related to increase the user commitment, since it is based on offering the user the possibility of playing a game or compete, something usually pleasant to their brain.

- **Guided competition:** This pattern is based on the fundamental mechanism of gamification: fostering competition against oneself, against other users or against the algorithm (automated competitor) to encourage the feeling of achievement. In many cases, setting very difficult objectives that require being connected for a considerable amount of time to win the proposed competitions or the game itself or paying for some kind of aid or advantage. Social networks often propose competitions and challenges. But this is a very extended pattern in all digital products. Role-playing is also an extended pattern within this category, when users do not compete as themselves but as fictional characters or avatars.

Example:

Imagine an online learning platform that displays a leaderboard showing the top-performing users based on points, badges or completion rates. User are encouraged to compete for higher rankings, which can motivate them to engage more often or with greater commitment. Economic rewards, direct (in the form of money) or indirect (in the form of gift cards, material prizes, virtual money) may be offered too.

Platform designers must strike a balance between competition and pressure to perform. They profile students depending on their habits (session length, learning schedule, learning frequency, preferences, performance history, etc.) and knowledge level to optimize all these features.

- **Grinding and mere-exposure:** This pattern requires users to perform easy or repetitive tasks, even only to be connected or exposed to some content, to obtain points, credits or some kind of reward. For example, a service gives extra lives to users if they watch ads. Many games have an automated mode that can be played without the user's intervention that improve player's situation or reputation (through rewards) only by keeping the game executing on the device.

Example:

Imagine a role-playing game on a farm. The player needs to feed the farm animals in the game repetitively to progress, seemingly for arbitrary reasons. Each game level forces the player to complete more feeding cycles before they can progress through the fun tasks involved in playing the game.

If the amount of required repetitive tasks is too large, or they are required too frequently, players can feel frustrated or lose interest. Game designers must strike a balance between hooking and boredom. They profile gamers depending on their habits (gaming session length, game schedule, game frequency, game preferences, etc.) to optimize all these features.

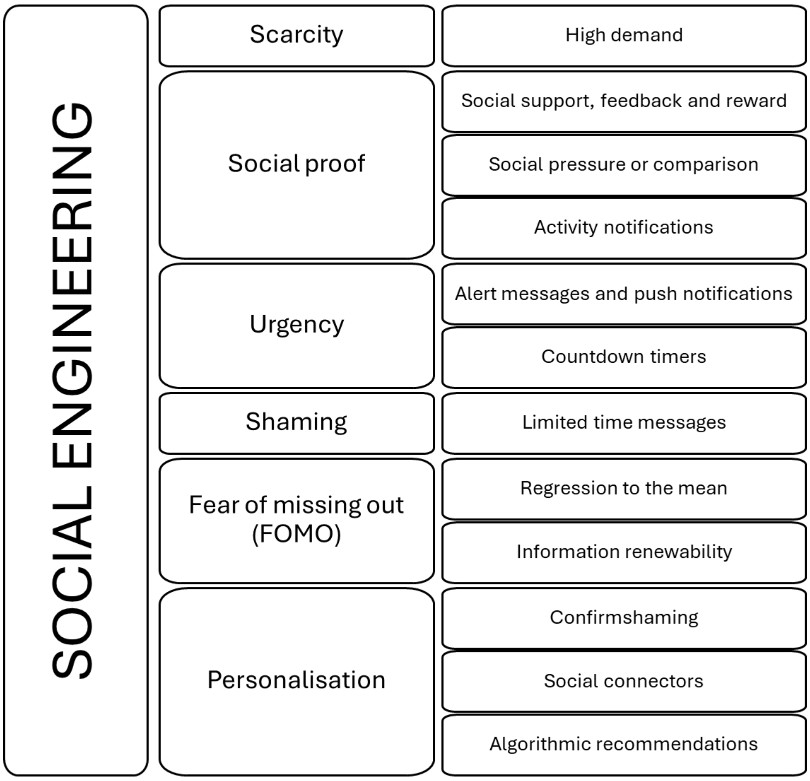
- **Endowment:** Every time users visit the platform or use the application or service, investing time there, they improve their situation or reputation (points, followers, trophies, level, etc.). This makes it very difficult for them to detach from the app or service, or even delete their account because they would lose all they have won to the moment. For example, if you delete your account on a social network, you will have to start from scratch if you sign in again in the future. Many games have specific points or locations that players must reach before they can safely save their progress (without losing their achievements) and stop playing (sometimes it is called “Can't Pause or Save” pattern in this context).
- **Periodic rewards:** Some platforms, applications and services give you a reward the first time you use them each hour, day or week, for example. On the other hand, if you do not connect in a specific period, you are penalized. In some cases, streaks are established and rewarded. For example, you have the “perfect week” if you use the application each day during a week.
- **Complete the collection:** This pattern is based on offering users something to collect, for example, badged, trophies, skins. In general, different kinds of objects or characters often with different associated values. Obtaining the 100% of collectable items implies a high degree of commitment or engagement with the application or service. Sometimes they are associated with points programs, which once obtained can be exchanged for objects from the collection. This pattern is often used in online videogames but also on learning or health apps. For example, when users complete a certain activity, they get a badge.

Attention capture

This approach is directly related to time, prolonging users’ sessions by engaging their attention by different methods.

- **Autoplay:** This pattern is based on playing songs or videos, or at least, short versions showing a summary, without users’ intervention. Usually, the autoplay begins the moment the user stops enough time on page, frame, link, etc. For example, this happens in many video streaming platforms and in social networks.

B. SOCIAL ENGINEERING



SOCIAL ENGINEERING	Scarcity	High demand
	Social proof	Social support, feedback and reward Social pressure or comparison Activity notifications
	Urgency	Alert messages and push notifications Countdown timers
	Shaming	Limited time messages
	Fear of missing out (FOMO)	Regression to the mean Information renewability
	Personalisation	Confirmshaming Social connectors Algorithmic recommendations

This high-level category consists of offering users something based on their cognitive biases or behavioural tendencies (anchoring, loss aversion, etc.) to manipulate them into making unintended, unwilling or even potentially harmful decisions.

Scarcity

This approach is related to time and commitment, based on creating a sense of limited availability, encouraging users to take immediate action.

- **High demand:** This pattern is based on showing substantial need or appetite for something from other users. The goal is encouraging rushed decisions and increased engagement by making users compelled to participate in something that many other users like: users tend to follow what others do. Many social networks display messages of limited availability or offer content only available by invitation.

Example:

Imagine a social network offering an exclusive content to a limited number of users. Some users may feel compelled to register as soon as they see how the number of available invitations decreases rapidly as time progresses, even if they weren't initially interested.

Designers must find the way to guarantee enough engagement. They profile the social network users depending on their habits and preferences to optimize all these features concerning dissemination (who receives the information, how and when) and the exclusive content itself (how often is it offered, what kind of content).

Social proof

This approach is related to time and commitment, based on creating illusions of popularity, credibility, consensus, endorsement or any indication that others find value or importance in what you're doing or sharing. Or their equivalent negative aspects.

- **Social support, feedback and reward:** This pattern is based on stimuli which instigate positive experiences involving other users including a plethora of verbal and non-verbal expressions or gestures such as a praise, a smile, a thumbs-up, an applause, good reputation and all its digital equivalents. For example, the "Like" button, the "Repost" and the "Heart" buttons, etc. Users can also send reactions to content, reply with messages or images, or make comments in almost all social networks. Or become followers. Lenses and filters offered as tool or functionality that enables appearance alteration, photo and video editing, "skins" generation for characters, etc. can also be categorized within this pattern.
- **Social pressure or comparison:** This pattern is again related to the first but, in this case, it appeals to the negative aspect of the social element. It is based on implicit competition, not directly proposed by the provider (as in Guided competition) but caused by the competitiveness that can be generated between users for having better social stats (more likes, followers, etc.). In almost all social networks, users can see, since they are usually public data by default, the followers who have other accounts or profiles, the comments and interaction they generate, etc.
- **Activity notifications:** This pattern is based on showing announcements of users' activity. For example, "Alice has a new post" in almost all social networks, or "Alice liked this post". In this case, this pattern is directly related to the first one in this category, since what is usually notified is the receipt of some type of social reward, in real time, so that its impact is amplified. But notifications can be also used to compare activity streaks with other users ("Bob is posting a lot this week") or to show users their lack of engagement ("You haven't posted in a while…"). A different type of activity notification is the one showed in real-time within messaging applications notifying users whenever their contact is typing ("…", "is typing"). Instant messaging apps use this pattern to keep users on the screen waiting for a response, for example.

Example:

Imagine a social network designed to produce activity notifications only for content updates in users' favourite accounts, or only for important content updates (with produced interaction above a threshold). But, perhaps, there are users who may be interested in knowing a slight change in the profile of someone they follow, in all new content, etc. Or they wish a "summary" notification.

Users are allowed to customize, in some respects, the type of notification they want to receive. The rest of the configuration is done automatically.

A high notification frequency may lead to a greater connection time or commitment among specific user groups (new users, young users, etc.). But other users may feel upset when they see many notifications.

Designers analyse user data showing behaviour, preference, preferred usage, or location, for example, for customizing notification content and frequency to obtain the desired results in all cases.

Urgency

This approach is related to time and commitment, it works on the idea of false urgency and loss aversion, impacting users' decision making under the pretext of emergency.

- **Alert messages and push notifications:** This pattern is based on proposing time-sensitive actions or displaying warning that exaggerate the consequences of not doing something to pressure users into taking specific actions. Almost all social networks use this kind of messages to alert users when they receive direct communication, for example.

> **Example:**
>
> Imagine a social network designed to produce, automatically, an alert message as a friend's birthday reminder.
>
> Designers analyse user contacts, gather their birth date, and decide the best moment to produce the alert message for this specific user. And if the alert is repeated when ignored the first time, the text included in the successive alerts, etc.

- **Countdown timers:** This pattern is based on the same principles that the previous one, but it shows backward counting in fixed units from an arbitrary starting number to mark the time remaining before an event. Different platforms, applications and services use this kind of timers before a flash sale, a live-stream or the expiration of a deadline as a streak that is broken if the user does not log in or complete a task.

> **Example:**
>
> Imagine a learning platform designed to show users a countdown timer with the time they have left to complete a lesson or pass a test if they do not want to lose a badge or any other reward at stake.
>
> A high use frequency of this pattern may lead to a greater connection time or commitment among specific user groups (new users, engaged students, etc.). But other users may feel upset when they see timers too often.
>
> Designers analyse user data showing behaviour, preference, preferred usage, or location, for example, for customizing the utilization of this pattern and obtain the desired results in all cases.

Shaming

This approach is related to time and commitment, it is based on inducing feelings of guilt or embarrassment in users.

- **Limited time messages:** This pattern is based on offering users a limited window opportunity to take specific actions. It may be related to High demand, Alert messages, Countdown timers or the patterns within the Fear of missing out category. But, in this case, when the window of opportunity is not taken advantage of, blame is mainly used with messages such as "Your friends have missed you", "Your followers have been waiting for your response", "You missed something important", etc.

Example:

Imagine a social network where messages and shared content are only available for a short time before they become inaccessible. If the recipient of this kind of ephemeral message does not read it or open it in time, the sender will know.

Designers analyse user data showing behaviour, preference, preferred usage, or location, for example, for customizing the utilization of this pattern and obtain the desired results in all cases. The main decision in this case is the optimum size of the time window for each user/content.

Fear of missing out

This approach (FOMO) is based on exploiting the anxiety or unease caused by the fear that others are experiencing something more important elsewhere. This fear drives users to stay connected constantly (approach related to time), fearing they might miss something important.

- **Regression to the mean:** This pattern is based on offering users the most popular or viral content at different times and locations, so that, even if they consume it repeatedly, it seems good to them because they are guaranteed not to miss it. Almost all social networks use this pattern, repeating specific content to be sure that users have the chance to see it and to pay enough attention.

Example:

Imagine a social network where the most popular content is offered among the rest of the contents, but it is repeated periodically, for example over 24 hours. And always labelled as a “trend”. In addition, there is a specific tab for this type of content that summarizes what is most popular on this network at this moment.

A good use of this pattern may lead to a greater connection time or commitment among specific user groups. But other users may feel upset or bored if they see the same content too often.

Designers analyse user data showing behaviour, preference, preferred usage, or location, for example, for customizing the utilization of this pattern and obtain the desired results in all cases.

- **Information renewability:** This pattern is based on constantly streaming content updates. The user perceives that in the time they spend disconnected, they will lose all those updates among which there will surely be interesting or important ones. Almost all social networks use this pattern, combined with Algorithmic recommendations to offer the proper content for each user.

Example:

Imagine a social network where users’ timeline is auto-refreshed each minute and a counter indicates the number of new posts or contents that has not been reviewed yet.

A good use of this pattern may lead to a greater connection time or commitment among specific user groups. But other users may feel overwhelmed by the information refreshing rate. Even by auto-refreshing, because if it is too fast, it may interrupt them when enjoying some content.

Designers analyse user data showing behaviour, preference, preferred usage, or location, for example, for customizing the utilization of this pattern and obtain the desired results in all cases. The main decisions in this case are the refreshment rate and the configuration of auto-refreshment by default. In addition, the inclusion of counters or labels drawing attention to new or unseen content.

Personalisation

The success of most patterns that depend on personal data is in customizing the parameterization of that pattern to find the perfect balance that makes the user stay connected for as long as possible with the highest possible degree of commitment without feeling annoyed by these patterns. Personalisation can be offered in different ways.

- **Confirm shaming:** This pattern is strongly related to the Shaming category, but it has been included here because it is based on manipulative personalisation, capitalizing emotional language (often combined with the Persuasive language pattern) and psychological pressure for a specific user confirming a specific action or task in a specific context. Different learning and health apps use this pattern, for example “Are you leaving so soon?” when the user session is shorter than usual. Social networks and online games also rely on this pattern.

Example:

Imagine an online game designed to make the player feel guilty or embarrassed when rejecting other players invitation to join them in a game.

Designers analyse user data showing behaviour, preference, preferred usage, or location, for example, for customizing the utilization of this pattern and obtain the desired results in all cases. The main decision is in which actions or tasks it is indicated to use the pattern and how to combine it with others, such as the one related to the use of language, to amplify its effects.

- **Social connectors:** This pattern is based on making online experiences more enjoyable by sharing with friends or family. Furthermore, some providers offer users a reward when they invite new users or link to them from their accounts (social pyramid schemes). Additionally, social connection amplifies the impact of patterns in the Social proof, Shaming and FOMO categories. Almost all social networks offer the functionality of retrieving users' contacts from their address books and from other networks or repositories. Also to locate them on the network, to invite them if they do not yet have an account. All these features are offered periodically so that online contacts are updated at the same pace as relationships in real life. Combined with Algorithmic recommendations, this pattern offers new contacts. And with Alert messages and push notifications, it notifies you when a contact you may be interested in joins the network, for example.

Example:

Imagine a social network designed to keep users in touch with their friends and family, so that day-to-day life, important events, etc. can be shared with all of them. To do this, both at the creation of the account and afterwards, it offers a multitude of static and dynamic mechanisms that allow the user to obtain data to locate friends and family on that same network.

The data necessary to locate the closest contacts of each user and allow their connection within the network.

- **Algorithmic recommendations:** This pattern is usually combined with many of the already mentioned, because it is based on personalising users' experiences to enhance their engagement. Therefore, algorithmic recommendations reinforce user behaviour, amplifying the impact of the rest of addictive patterns. Recommendations are often based on past behaviour, users' profile (habits, preferences) and trending topics. Their goal is to recommend content, social connections or specific activities. Before the introduction of algorithmic recommendations users had to autonomously explore platforms, applications and services, finding for themselves the functionalities, contacts or contents they liked most. Algorithmic recommendations heavily influence users' decision-making, with a special focus on time and commitment. This is the pattern that makes the most intensive use of personal data, since the more providers know about the user, in all possible dimensions, the more tailored (to their taste) the recommendations will be and the more effective they are in increasing connection time and degree of commitment. All social networks use this type of algorithmic recommendation, also streaming platforms, online learning services, etc. Different recommendation algorithms try to optimize different engagement metrics[36]: weighted averages of all the types of interaction that a content can have; expected watch time, a combination of liking, commenting, and play time, etc. For example, a recommender may show contents predicted to be very likely that the user like the moment it is predicted that the user is going to log out trying to extend the session.

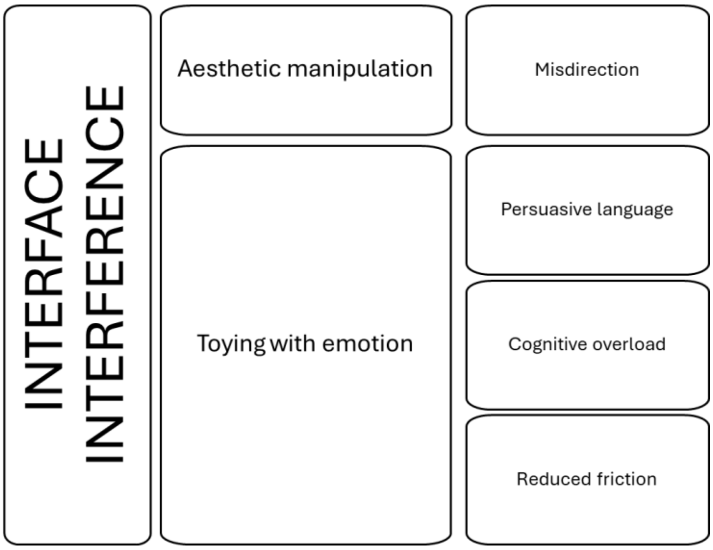
Example:

Imagine a social network where users see posts and content recommended by an algorithm, predicted as the content they will like best.

Designers define an engagement metric and try to optimize its value offering each user, with all the possible knowledge accumulated about him or her, those contents that predicts maximum engagement.

[36] Narayanan, A. (2023). Understanding Social Media Recommendation Algorithms https://academiccommons.columbia.edu/doi/10.7916/khdk-m460

C. INTERFACE INTERFERENCE



This high-level category consists of manipulating the user interface to privilege specific actions over others, to draw the user's attention to specific content or activities.

Aesthetic manipulation

This approach is based on altering the visual design to mislead users, emphasizing certain elements while downplaying others. This can be used to keep users logged in longer or to increase their commitment.

- **Misdirection:** This pattern is based on using colour, font or layout to manipulate users' behaviour, focusing their attention on one very specific item in every moment. This pattern is commonly used to help others succeed, drawing the user's attention to elements related to FOMO, Personalisation, etc. Something common is to modify the interface's design with high frequency to make the user pay attention to new functionalities or those that most interest the provider at that moment. In addition, many providers intentionally omit the concept of time when users are connected to their platforms, applications or services, for example, not showing clocks with the time or the date.

Toying with emotion

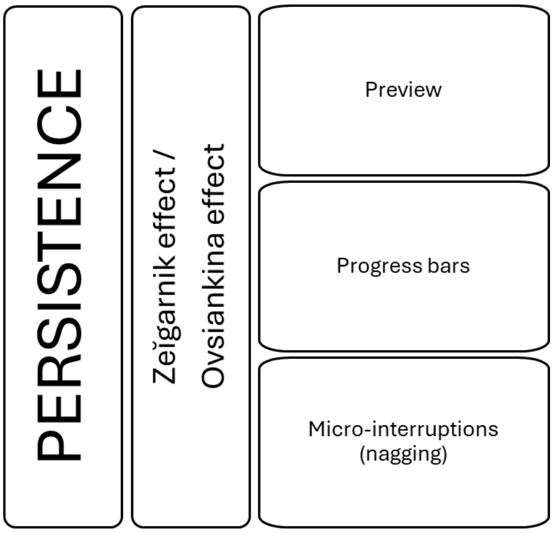
This approach is based on exploiting user's psychological vulnerabilities regarding their feelings and emotions. This approach can be related to time or to commitment.

- **Persuasive language:** This pattern is based on the use of words, sentences or communication techniques well-known for the capability of influencing individuals' thoughts, emotions or actions. Examples of persuasive language include emotional pressure ("Connect now!"), misleading promises ("This makes you a better person") or choice farming ("Post now" vs "Continue without posting").
- **Cognitive overload:** This pattern is based on overwhelming the user with too much information, content and distractions, with too many options simultaneously, influencing their cognitive capacity. This makes it easier for them to lose track of time or the ability to assess the consequences of their decisions. For example, almost all social networks

offer visual effects such as filters, lenses, stickers, etc. It can be considered Personalisation too, but for most users, the connection time is extended by this other effect of cognitive overload.

- **Reduced friction:** This pattern is based on making the use of platforms, applications and services easy and smooth. Specifically, regarding processes that keeps users connected or increase their commitment.

D. PERSISTENCE



This high-level category consists of exploiting the innate human urge to finish initiated tasks.

Zeĭgarnik effect/Ovsiankina effect

This approach is based on the user perceiving that they have unfinished tasks, helping to generate some discomfort in them because these tasks remain in their brain for longer than in the case of finished tasks. These effects can be exploited to increase users' connection time and commitment.

- **Preview:** This pattern is based on allowing users start to consume the content or the article. Then, they wish to complete the task, a certain tension is generated in them until they do not do it.
- **Progress bars:** This pattern is based on letting users know how close they are to completing a task. Once they know that something is "half-done", they are more likely to spend the time required to finish.
- **Micro-interruptions (nagging):** This pattern is based on using ads, messages, pop-ups, suggestions, etc. They can cause users to suffer micro-interruptions during their connection that make them jump from one site or content to another. And at some point, need to recover the path followed to finish consuming all the content or the tasks left unfinished before.

IV. IMPLICATIONS FOR DATA PROTECTION

The preceding sections' analysis presents how personal data processing across numerous platforms, applications, and services includes specific operations to increase connection time or level of commitment, influencing users' decisions, using personal data for such purposes or generating new personal data and addressability. All those operations point to different implications for data protection which are discussed below in this section.

As previously mentioned, the longer the connection time and level of commitment, the more personal data the provider can collect. This means that, in addition to some addictive patterns being fuelled by personal data, including such operations in the design of the personal data processing (performed to provide digital services and products) may result in gathering more personal data and with a greater scope.

The personal data processing carried out by the platform, application or service provider is specified in the terms and conditions of the service and in its privacy policy and has one or more legal bases that make it lawful. The operations related to addictive patterns occur within the framework of this processing. Addictive patterns are not implemented in isolation, but rather involve additional operations that determine the way the global processing is carried out, so that it lasts over time, so that it gathers more data, so that it conditions the user’s decision, etc. Among their consequences, new risks are generated for the rights and freedoms of users or existing ones are aggravated.

Table 1 summarises the classification of addictive patterns proposed in the previous section. For each pattern, an estimation of the intensity of personal data consumption, the capacity to collect or infer personal data, and the potential GDPR infringements are provided.

In developing this table, the concept of Personal Data Consumption Intensity has been introduced as the degree or extent to which a specific pattern relies on personal data to achieve its objectives. NA means Not Applicable, because this pattern does not need to process personal data to work correctly; the symbols +, ++ and +++ have been used to indicate low, medium and high intensity respectively. It can be observed that patterns within the Forced Action and Social Engineering categories consume users' personal data to achieve their goals. Some of them are very intensive, as is the case with Algorithmic Recommendations.

The personal data processed in this context of addictive patterns can be of four types:

- **Provided actively or directly by the user:** User data mentioned in section II, information provided when creating an account, when writing a profile, through a contact form, etc. such as name, age, gender or email address.
- **Provided passively or indirectly by the user:** Connection fingerprint mentioned in section II, information provided during the interaction with the platform, application or service concerning devices, browsers, IP addresses or geolocation. But also, User behaviour and User habits and preferences such as content created, shared or liked, contacts made or given consents, session lengths, days and hours, etc.
- **Provided by external sources:** User data, User behaviour or User habits and preferences coming from off-platform third parties, for example, from data brokers or data management providers.
- **Inferred by the provider:** Assumptions and interpretations derived from the three previous data categories with statistical inference, machine learning or Artificial Intelligence methods, for example.

High-level pattern	Meso-level pattern	Low-level pattern	Personal Data Consumption Intensity	Capacity to collect or infer personal data	Potential GDPR infringements
FORCED ACTION	Forced continuity	Pull to refresh	NA	Provided actively or directly by the user. Provided passively or indirectly by the user. Provided by external sources. Inferred by the provider.	Accountability. Data protection by design and by default. Transparency. Lawfulness. Fairness. Purpose limitation. Data minimisation. Processing of special categories of personal data. Automated individual decision-making, including profiling.
		Endless scrolling	NA		
		Endless streaming	NA		
		Timers	+		
		Playing by appointment	+		
	Gamification	Guided competition	+		
		Grinding and mere-exposure	+		
		Endowment	NA		
		Periodic rewards	NA		
		Complete the collection	NA		
	Attention capture	Autoplay	NA		
SOCIAL ENGINEERING	Scarcity	High demand	++		
	Social proof	Social support, feedback and reward	NA		
		Social pressure or comparison	NA		
		Activity notifications	++		
	Urgency	Alert messages and push notifications	++		
		Countdown timers	++		
	Shaming	Limited time messages	++		
	Fear of missing out	Regression to the mean	++		
		Information renewability	++		
	Personalisation	Confirmshaming	++		
		Social connectors	++		
		Algorithmic recommendations	+++		
INTERFACE INTERFERENCE	Aesthetic manipulation	Misdirection	NA		
	Toying with emotion	Persuasive language	NA		
		Cognitive overload	NA		
		Reduced friction	NA		
PERSISTENCE	Zeĭgarnik effect/ Ovsiankina effect	Preview	NA		
		Progress bars	NA		
		Micro-interruptions (nagging)	NA		

Table 1. Addictive patterns classification and aspects concerning data protection

Some of these types are not only processed as input to addictive patterns but also occur as an output or result of said patterns. Thanks to the reactions observed in the user to certain design features or to a higher connection time or degree of commitment, the provider may be able to collect or infer data that it would not otherwise have been able to collect or infer. It is a direct result of the use of addictive patterns.

The column "Capacity to collect or infer personal data" in Table 1 reflects this output or result. For example, if Forced Action patterns are analysed, a user can directly provide personal data to the provider to participate in a flash sale, receive a periodic reward, or complete a collection. The user can also provide them indirectly; for example, the provider can collect their reading speed by analysing how they interact with a Pull to refresh or Endless scrolling pattern. An external source can provide data to a provider, for example, through an AutoPlay pattern, about the content the user is most interested in or the times when they are most willing to consume certain types of content. As for the provider, a pattern based on Timers may enable inferences about a user's patience or capacity for frustration and a Guided Competence pattern about their aggressiveness or competitiveness. At the same time, scheduled content (Playing by Appointment) can allow the provider to infer when the user is most available.

Aspects included in the "Potential GDPR infringements" column are developed in detail below. It can be determined, in general, that data protection regulations, specifically the GDPR, establish that the specific purposes for which personal data are processed should be explicit and legitimate and determined at the time of the collection of the personal data. The processing of an individual's personal data by the provider of a platform, application or service of which he or she is a user to increase the probability of success of addictive patterns must be framed in the global processing of personal data that that provider carries out within the relationship they have established. The operations that feed addictive patterns with personal data or that collect or infer data thanks to them are only a subset of all those that form part of said global processing. These specific operations' aim cannot be considered a legitimate one because it implies violating users' fundamental rights and freedoms, such as human dignity or integrity of the person (physical and mental) or right to liberty. It must be considered that data processing within addictive patterns may undermine individual autonomy, agency and freedom.

A. ACCOUNTABILITY

Article 24(1) of the GDPR establishes that the data processing controller shall implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation, in particular, taking account the risks of varying likelihood and severity for the rights and freedoms of natural persons.

The EDPB already established that "Article 35 refers to a likely high risk "to the rights and freedoms of individuals". As indicated in the Article 29 Data Protection Working Party Statement on the role of a risk-based approach in data protection legal frameworks, the reference to "the rights and freedoms" of data subjects primarily concerns the rights to data protection and privacy but may also involve other fundamental rights such as freedom of speech, freedom of thought, freedom of movement, prohibition of discrimination, right to liberty, conscience and religion"[37]. In addition, "The risk-based approach goes beyond a narrow "harm-based-approach" that concentrates only on damage and should take into consideration every potential as well as actual adverse effect, assessed on a very wide scale

[37] Article 29 Data Protection Working Party "Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679". https://ec.europa.eu/newsroom/article29/items/611236

ranging from an impact on the person concerned by the processing in question to a general societal impact (e.g. loss of social trust)"[38].

Furthermore, the EDPB pointed out the risks to the data subjects' rights and freedoms posed by all deceptive patterns in their guidelines. Specifically, the EDPB stated that "it is essential to keep in mind that deceptive design patterns raise additional concerns regarding potential impact on children and also other vulnerable groups of people"[39]. The AEPD research about addictive patterns based on a systematic review of the existing scientific evidence also raises concerns about the risk for all the users that addictive patterns could imply, but the heightened risk that may pose for such specific groups. Such risks must be addressed, and they can hardly pass the required assessment of necessity and proportionality as laid down in Article 35(7)(b) of GDPR.

The risks to the right to physical and mental integrity are the most obvious, but they are not the only ones. Other rights could be at risk due to the addressability necessary for the addictive patterns' operation.

The EDPB Guidelines 8/2020 on the targeting of social media users[40] already made a first analysis of the possible risks to the rights and freedoms of people without offering an exhaustive list in section 3. The guide established that targeting social network users may involve uses of personal data that go against or beyond individuals' reasonable expectations and, thereby, infringes applicable data protection principles and rules, and may involve an inference of interests or other characteristics, undermining control over their personal data, in addition to undermining, complicating or hindering the exercise of the rights of the interested parties. It detailed the possibility of discrimination and exclusion with discriminatory effects related to a person's racial or ethnic origin, health status or sexual orientation, or other protected qualities of the individual concerned. It also referred to the possible manipulation of users, since targeting mechanisms are used, by definition, to influence people's behaviour and choices, from purchasing decisions as consumers or in terms of their political decisions. It points out that even some targeting strategies can undermine individual autonomy and freedom and could be used to direct specific messages to the person and at specific times to which they are expected to be more receptive and thus surreptitiously influence their thought process, their emotions and their behaviour, and can be used to improperly influence people when it comes to political speech and democratic electoral processes, including disinformation activities or messages. In the same vein, the use of algorithms to determine what information is shown to which people can negatively affect the likelihood of accessing diversified sources of information in relation to a specific topic. This may in turn have negative consequences for the pluralism of public debate and access to information, in relation to the risks related to the so-called "filter bubbles" and those of "information overload". The targeting of social media users on the basis of information concerning their browsing behaviour or other activities outside the social media platform can give individuals the feeling that their behaviour is systematically being monitored. This may have a chilling effect on freedom of expression, including access to information, and can lead to self-censorship. The potential adverse impact of targeting may be considerably greater when it involves vulnerable categories of individuals, such as children. Targeting can influence the configuration of minors' personal preferences and interests and ultimately affect their autonomy and their right to development.

[38] Paragraph 11, Article 29 Data Protection Working Party "Statement on the role of a risk-based approach in data protection legal frameworks". Adopted on 30 May 2014. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp218_en.pdf

[39] EDPB Guidelines 03/2022 on Deceptive design patterns in social media platform interfaces: how to recognise and avoid them. Version 2.0. Adopted on 14 February 2023 https://www.edpb.europa.eu/system/files/2023-02/edpb_03-2022_guidelines_on_deceptive_design_patterns_in_social_media_platform_interfaces_v2_en_0.pdf

[40] EDPB Guidelines 8/2020 on the targeting of social media users Version 2.0 Adopted on 13 April 2021. https://www.edpb.europa.eu/system/files/2021-04/edpb_guidelines_082020_on_the_targeting_of_social_media_users_en.pdf

In the same Article 24(1) is required not only to ensure, but to be able to demonstrate compliance. Providers offering digital platforms, applications and services have all the information necessary to understand addictive patterns, how they work, which personal data they use, and what their impacts on users. However, they usually do not share this knowledge[41], forcing regulators, authorities and researchers to find workarounds to identify, analyse, and understand these patterns by asking users, instrumenting real products (often through closed APIs), or imitating these products using controlled experimental setups.

B. DATA PROTECTION BY DESIGN AND BY DEFAULT

Providers who enable addictive patterns are failing to comply with their Data Protection by Design and by Default obligation, as outlined in Article 25 of the GDPR. This article states that controllers shall implement appropriate technical and organisational measures taking into account the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, and other circumstances like the context and the scope, for example, that such processing affects children.

Implementing deceptive and addictive patterns in a processing is then a design decision that directly violates the principle of data protection by design and by default. Consequently, providers would fail to fulfil their core obligation to incorporate appropriate measures and necessary safeguards that effectively implement the data protection principles, thereby ensuring the protection of data subjects' rights and freedoms by design and by default.

The potential adverse impact of addressability may be considerably more significant where groups that must be specifically protected are concerned, such as children, elderly or persons with disabilities[42]. All these groups could see their rights violated to a greater degree by the data processing involved in addictive patterns.

C. TRANSPARENCY

The principle of transparency is laid down in Article 5(1)(a) of the GDPR. However, providers often fail to be transparent, open, or clear with users regarding how they will process their personal data to improve the performance of addictive patterns or address them using such patterns[43]. Commonly, the user is not informed of the additional processing purposes (to feed addictive patterns or to obtain profit from them), the potential risks for the rights and freedoms (recital 39 of the GDPR), the existence of automated decision-making, including profiling, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject (Article 13(2)(f) and Article 14(2)(g) GDPR).

As a result, users may not fully comprehend the implications of such processing and may be unable to exercise their rights enshrined in Articles 15 to 22 and to fulfil consent conditions, mainly when they are children or young.

[41] With the implications for the controller in relation to articles 58(1)(a) and 83(5)(e) of the GDPR.

[42] Articles 24, 25 and 26 of the Charter of Fundamental rights of the European Union.

[43] Sentence of the Court of Justice of the European Union. Schufa Holding (C-634/21): The Court points out that the data subject should be informed about the general logic of the processing (art. 15, par. 2 letter h)). But the Court remains silent on the possible reconciliation between the right to information and commercial secrets and/or intellectual property, while specifying that the information must be limited to offering an understanding of that logic and not complete knowledge (a circumstance that vice versa would prevent the accessibility of the processing).

The distinction between the different types of data that a provider can collect or infer is essential when determining the roles in each processing (controller, processor) and, therefore, the obligations that these roles imply regarding transparency or the exercise of data protection rights. For example, to fulfil the requirements of Article 15(1) GDPR and to ensure full transparency, providers should implement mechanisms for data subjects to check all their personal data, including those provided by external sources or inferred, sources and methods. The data subject is entitled to learn the data used as input for the different addictive patterns and the other information required by Article 15 GDPR.

D. Lawfulness

Personal data processing must be lawful to comply with the GDPR. This means that personal data should be processed based on the data subject's consent or some other legitimate basis (article 6). This means that personal data must be processed on one of the bases set out in Article 6 of the GDPR. Among those established in said article, those that could initially be considered for the lawfulness of including addictive patterns in personal data processing are the data subject's consent, the performance of a contract to provide a service or the legitimate interests pursued by the controller.

However, the data subject's consent would not be valid if it is not properly informed, if the consent for additional processing operations (such as addictive operations) is not provided by a clear affirmative act (recital 32 of the Regulation), if the performance of the contract including the provision of the service is subject to consent to the processing of personal data that are not necessary for the execution of said contract[44], or if the consent does not comply with article 8 GDPR on the conditions applicable to child's consent in relation to information society services.

If the processing is necessary for the performance of a contract to provide a service, in which it is alleged that the addictive patterns are an inherent part of it, article 6(1)(b) GDPR only applies when the processing in question is objectively necessary for the performance of the contract with the data subject. Or the processing must be objectively necessary for the application[45]. This article does not cover useful processing, but not objectively necessary to perform the service that is the subject of the contract or to apply the relevant pre-contractual measures at the request of the data subject, even if they are necessary for the other commercial purposes of the controller[46]. The expression "necessary for performance" clearly indicates that a mere contractual clause is not enough[47].

To the extent that such operations are not necessary, or violate data protection regulations, they could not be considered lawful[48]. Digital service contracts may incorporate clauses that expressly impose additional conditions on advertising, payments or cookies, among other issues. However, contracts cannot artificially expand the categories of personal data or the types of processing operations that the controller needs to carry out for the performance of the contract[49]. A relevant factor could be, for example, that the data subject

[44] Article 7.4 of the GDPR.

[45] Paragraph 22, EDPB Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects. Version 2.0, 8 October 2019. https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-22019-processing-personal-data-under-article-61b_en

[46] Paragraph 27, same guidelines.

[47] Paragraph 25, same guidelines.

[48] Paragraph 13, same guidelines. As a matter of lawfulness, contracts for online services must be valid under the applicable contract law. To ensure compliance with the fairness and lawfulness principles, the controller needs to satisfy other legal requirements. For example, for consumer contracts, Directive 93/13/EEC on unfair terms in consumer contracts (the “Unfair Contract Terms Directive”) may be applicable.10 Article 6(1)(b) is not limited to contracts governed by the law of an EEA member state.

[49] Paragraph 31, same guidelines.

was a minor. In this case (and apart from compliance with the requirements set out in the GDPR, including the "specific protections" that apply to minors), the controller must ensure that it complies with the relevant national regulations on the minor's capacity to enter into contracts[50].

The EDPB confirms that content personalisation may (although not always) constitute an intrinsic and foreseeable element of certain online services and, therefore, may in certain cases be considered necessary for the performance of the contract with the service user. Whether such processing can be considered an intrinsic aspect of an online service will depend on the nature of the service provided, the expectations of the average data subject, not only in light of the conditions of the service, but also in view of the way in which it is promoted, and the possibility of providing the service without personalising it. When the personalisation is not objectively necessary for the purposes of the underlying contract (for example, when the personalised content offered is intended to increase the use of the service by the user but is not an essential part of the use of the service), data controllers should consider the possibility of using an alternative legal basis, where appropriate[51].

Finally, the processing could be considered necessary for the legitimate interests pursued by the controller. Such legitimate interests exist, for example, where there is a relevant and appropriate relationship between the data subject and the controller, such as when the data subject is a controller client. However, the interests and fundamental rights of the data subject override the data controller's interests. The processing of personal data for addictive purposes or as a result from addictive behaviours provoked by the own provider cannot be considered a legitimate interest.

E. FAIRNESS

The principle of fair processing laid down in Article 5(1)(a) of the GDPR is the starting point for assessing the existence of addictive design patterns. As the EDPB already stated, fairness is an overarching principle that requires that personal data shall not be processed in a way that is detrimental, discriminatory, unexpected, or misleading to the data subject[52]. The fairness principle includes, among others, the recognition of reasonable expectations of the data subjects, the consideration of the possible adverse consequences that the processing may have on them and the consideration of the relationship and the potential effects of the imbalance between them and the data controller[53].

Concerning fairness, providers often use addictive practices to process users' data in ways that contradict their reasonable expectations and may involve unexpected or undesired uses of personal data. This may include manipulative language or designs. Additionally, addictive patterns could have detrimental and harmful effects on the users, in particular regarding the risk to the fundamental right to physical and mental integrity[54].

[50] Paragraph 13, EDPB Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects. Version 2.0, 8 October 2019. https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-22019-processing-personal-data-under-article-61b_en

[51] Paragraph 57, same guidelines.

[52] EDPB Guidelines 4/20219 on Article 25 Data Protection by Design and by Default, version 2.0, adopted on 20 October 2020 https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_en.pdf

[53] Paragraph 12, EDPB Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects. Version 2.0, 8 October 2019. https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-22019-processing-personal-data-under-article-61b_en

[54] Charter of fundamental rights of the European Union, Article 3 Right to the integrity of the person (1) Everyone has the right to respect for his or her physical and mental integrity.

As data subjects, they are often not given enough autonomy or agency to determine how their personal data is used, or the scope and conditions of data processing. In some cases, users may be unfairly locked into using platforms, applications, and services that feature addictive patterns, which can limit their ability to use alternative versions free of these patterns. As mentioned before, data processing involved in addictive patterns may entail merging personal data from external sources with data provided to the provider's platform, application, or service and deriving inferences. As a result, personal data might be utilised for purposes beyond the original and in ways that individuals could not reasonably have foreseen.

The fairness principle has an umbrella function, and all addictive patterns cannot comply with it regardless of compliance with other data protection principles[55].

F. PURPOSE LIMITATION

The purpose of data collection must be identified clearly and concretely: it must be sufficiently detailed to determine which processing activities are and are not included in the explicitly specified purpose and to allow the evaluation of compliance with regulations and the application of guarantees relating to data protection. For these reasons, vague or general purposes, such as "improving user experience", "marketing purposes", "security purposes", or "future research", typically do not satisfy - without providing a greater degree of detail – the “specificity” criterion[56].

Therefore, the purpose limitation principle in article 5(1)(b) GDPR could not be fulfilled in the context of addictive patterns since the data processed by addictive features are not collected for specified, explicit or legitimate purposes.

G. DATA MINIMISATION

For the same reason, it may be challenging to fulfil the data minimisation principle in article 5.1(c), since the data actually processed are often not adequate, relevant or limited to what is necessary for the declared purpose. It is important to note that one of the primary goals of providers when using these patterns is to keep users engaged for longer or with a higher level of commitment to gather more personal data about them.

H. PROCESSING OF SPECIAL CATEGORIES OF PERSONAL DATA

The processing of personal data that reveals racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited by Article 9(1) of GDPR and such prohibition only could be lifted in certain circumstances lay down in Article 9(2) of GDPR. Most of the data processing that feeds addictive patterns looks for weaknesses or vulnerabilities of users that have to do with their state and mental health without any of the conditions required for lifting this prohibition being fulfilled.

[55] Based on the same reasoning developed in the EDPB Guidelines 03/2022 on Deceptive design patterns in social media platform interfaces: how to recognise and avoid them.

[56] Pages 15 and 16, Article 29 Data Protection Working Party “Opinion 03/2013 on purpose limitation”. Adopted on 2 April 2013. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf

Furthermore, Article 9(2) does not recognise “necessary for the performance of a contract” as an exception to the general prohibition on processing special categories of personal data.[57]

To the extent that data processing that implements addictive patterns infers data relating to health, for example, eating disorders, it would also involve the processing of special categories of data. This fact would occur regardless of the inference method or whether this inference was correct or not, in the latter case it would also imply a problem regarding the accuracy of the data. The same could be concluded in relation to any special category of data.

Article 9(2)(e) of the GDPR allows the processing of special category of data in cases where the data have been manifestly made public by the data subject. The EDPB states that “The word «manifestly» implies that there must be a high threshold for relying on this exemption” and provides guidance on the elements that need to be considered for controllers to demonstrate that the data subject has clearly manifested the intention to make the data public[58].

I. AUTOMATED INDIVIDUAL DECISION-MAKING, INCLUDING PROFILING

Automated decision-making should also be carefully assessed in this context, given that according to Article 22 of GDPR, users "have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her".

Even if the decision-making process does not produce legal effects, it could still fall within the scope of Article 22 if it produces an equivalent or significantly similar effect in its consequences. For data processing to significantly affect a person, the effects of the processing must be significant enough to be worthy of attention. In other words, the decision must have the potential to:

- significantly affect the circumstances, behaviour or choices of affected persons;
- have a prolonged or permanent impact on the data subject; either
- in the most extreme cases, cause the exclusion or discrimination of individuals[59].

As already mentioned, the scale at which addictive patterns are applied forces providers to automate them as much as possible to make them profitable. Furthermore, as has also been noted, there may be impacts on physical and mental integrity or they can cause discrimination, exclusion and manipulation, undermine individual autonomy, influence users’ thought processes, emotions and behaviour, limit their freedom of information and expression, generate self-censorship and affect the autonomy and development of minors. In this regard, recital 71 of the GDPR about automated individual decisions must be highlighted, since it explicitly states that “Such a measure must not affect a minor”[60].

[57] Page 22, Article 29 Data Protection Working Party “Guidelines on consent under Regulation 2016/679”. Adopted on 28 November 2017. As last Revised and Adopted on 10 April 2018. https://ec.europa.eu/newsroom/article29/items/623051/en

[58] EDPB Guidelines 8/2020 on the targeting of social media users Version 2.0 Adopted on 13 April 2021. https://www.edpb.europa.eu/system/files/2021-04/edpb_guidelines_082020_on_the_targeting_of_social_media_users_en.pdf

[59] Section IV.B, Article 29 Data Protection Working Party “Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679”. Adopted on 3 October 2017. As last Revised and Adopted on 6 February 2018. https://ec.europa.eu/newsroom/article29/items/612053/en

[60] Paragraphs 9 to 18, EDPB Guidelines 8/2020 on the targeting of social media users Version 2.0 Adopted on 13 April 2021. https://www.edpb.europa.eu/system/files/2021-04/edpb_guidelines_082020_on_the_targeting_of_social_media_users_en.pdf

Failure to comply with the provisions of article 22, and, where applicable, with the provisions of articles 13(2)(f) and 14(2)(g), could mean that the processing fails to comply with the principles of lawfulness, fairness and transparency.

V. CONCLUSION

Providers that offer platforms, applications and services process the personal data of their users. In many cases, the business model of these providers leads them to try to lengthen the sessions of these users when using their products or to increase their level of commitment and the amount of personal data that is collected about them. All these factors could positively impact the return on investment made in developing and maintaining digital products that are theoretically offered for free or at a significantly reduced price. For this reason, some providers include additional operations in the processing of their users' personal data to implement deceptive and addictive design patterns whose objective is to manipulate their activities and decisions.

The European Data Protection Board has already addressed deceptive patterns in the document "Guidelines 03/2022 on deceptive design patterns in social media platform interfaces: how to recognise and avoid them". These guidelines focused on such patterns for social media use cases.

Within the framework of its obligations, the AEPD has carried out a systematic review of the existing scientific evidence about addictive patterns on different platforms, applications, and services (social networks, but also video or music platforms, adult content, games, learning environments, health and well-being applications, etc.), which means addressing new use cases from a complementary perspective. In this way, the EDPB guidelines can be completed through a unified approach to deceptive and addictive patterns.

This report defines addictive patterns as design features, attributes, or practices that determine a particular way of using digital platforms, applications, and services intended to make users spend much more time using them or with a greater degree of commitment than what is expected, convenient, or healthy for them.

The conducted analysis shows how users' personal data processing on numerous platforms, applications, and services includes specific operations, all of which are deceptive, to increase their connection time or their level of commitment to influence their decisions. Their personal data are being used for this purpose or to generate new data and perform addressability, as it allows addictive strategies to be personalised to a very low-level degree.

In this document, a classification of addictive patterns has been proposed following a three-level ontology (high, medium, low). The so-called high-level patterns are general strategies independent of the context and the application, four of them have been identified: Forced action, Social engineering, Interface interference, and Persistence. Mid-level patterns describe more specific approaches exploiting specific users' psychological weaknesses or vulnerabilities. Finally, low-level patterns correspond to the particular execution of different approaches and are often context- or application-specific.

All these patterns may require personal data as input, collect or generate new personal data, or influence user behaviour and decision-making in the context of personal data processing.

The incorporation of operations that implement addictive patterns to the processing of personal data has important implications for different aspects related to data protection, such as accountability, the effective application of data protection obligations from the data protection by design and by default principle, transparency, lawfulness, fairness, purpose limitation, data minimisation, the processing of special categories of data or automated individual decision-making. It also implies a risk to the rights and freedoms of all users. In particular, to the right to their physical and mental integrity. But they can also cause discrimination, exclusion and manipulation, undermine individual autonomy, influence individuals' thought processes, emotions and behaviour, limit their freedom of information and expression, generate self-censorship and affect autonomy and development. These consequences can be severe for children and young users.

The set of patterns described in this document is not exhaustive. New patterns dependent on the context and the platform, application, or service could be found, or different ones could be created. Furthermore, the patterns already identified will evolve in the future. Therefore, it is necessary to continue developing this type of review of the available evidence and subsequent analyses to protect users in the digital environment effectively.