User Autonomy and Algorithmic Recommendations under the Digital Services Act, the Digital Markets Act, and the Political Advertising Regulation*

Anna Vicinanza

Table of contents

1. Introduction

Algorithmic recommender systems play a central role in shaping online experience. The information-abundant environment of the Internet paved the way for the success of digital services consisting of content organisation.[1] Access to information has thus become increasingly intermediated by large platforms,[2] which systematically sort information according to

* Peer-reviewed article

[1] T. Gillespie, *Custodians of the Internet: Platforms, Content Moderation, and the Hidden Decisions That Shape Social Media*, New Haven, 2018, esp. 13; L. D. Introna – H. Nissenbaum, *Shaping the Web: Why the Politics of Search Engines Matters*, in *The Information Society,* 16(3), 2000, 169 ff.

[2] A. Bradford, *Digital Empires: The Global Battle to Regulate Technology*, New York, 2023, esp. 6; J. E. Cohen, *Between Truth and Power: The Legal Constructions of Informational Capitalism*, Oxford,

various criteria that do not reflect the chronological order of upload, but rather alignment with individual user preferences, popularity, and paid advertising.

While the organisation of information based on relevance and sponsoring was already performed by traditional media, digital platforms differentiate their selection for each individual, thanks to technologies allowing the targeted recommendation of content. These are "recommender systems", defined as automated systems suggesting or prioritising specific information to users on online platforms.[3] Personalised recommendations have not always been a central feature of platforms,[4] but gradually emerged with the development of their business model, which combines the dynamics of the "attention economy",[5] with those of "surveillance capitalism".[6]

The attention economy characterises all advertising-driven businesses, including the media sector. They are described as operating within a multi-sided market,[7] where on one side are the users, who access the service for free, and on the other are advertisers, who pay to have their content shown. Advertising thus constitutes the primary revenue stream for most of these services. Since the value of advertising space is determined by its capacity to reach the attention of an audience, platforms' efforts focus on generating user engagement, to subsequently sell it to the highest bidder,[8]

2019, esp. 41.

[3] DSA, art. 3(s): a «fully or partially automated system used by an online platform to suggest in its online interface specific information to recipients of the service or prioritise that information, including as a result of a search initiated by the recipient of the service or otherwise determining the relative order or prominence of information displayed».

[4] For instance, Facebook presented news in a reverse chronological order from 2006 to 2009, and Twitter and Instagram incorporated algorithmic filtering only in 2016, after respectively 10 and 6 years of activity. See: P. Napoli, *Social Media and the Public Interest. Media Regulation in the Disinformation Age*, New York, 2019, esp. 34. Until 2009, Google presented content based on relevance but without personalised results. See: E. Pariser, *Il Filtro*, Milan, 2012.

[5] T. Wu, *Is the First Amendment Obsolete?*, in *Michigan Law Review*, 117(3), 2018, esp. 555; P. Napoli, *Social Media and the Public Interest. Media Regulation in the Disinformation Age*, cit., esp. 34.

[6] S. Zuboff, *Il capitalismo della sorveglianza*, Rome, 2019.

[7] However, this conceptualisation is not universally accepted. For instance, Newman suggests a different model in which users are not simply one side of the market, but rather the producers – of attention – while digital intermediaries act as distributors, and advertisers are the true end clients. See: J. M. Newman, *Antitrust in Attention Markets: Definition, Power, Harm*, in *University of Miami Legal Studies Research,* Paper No. 3745839, 2020.

[8] How real-time bids work is described in: E. Izyumenko et al., *Online Behavioural Advertising, Consumer Empowerment and Fair Competition: Are the DSA Transparency Obligations the Right Answer?*, in *EuCML*, 14(2), 2025, esp. 3.

whether commercial advertisers, governments, or political parties.[9]
It is in this double transaction – attracting users' attention and selling it to advertisers – that the functioning of any recommender system is grounded. However, while this double transaction also characterises traditional media markets, platforms possess a technological advantage in generating user engagement and segmenting the market for advertising purposes: algorithmic recommender systems enable the constant analysis of user data, alongside continuous experimentation and optimisation, to predict which content an individual user is most likely to engage with and to generate targeted recommendations accordingly.[10] In this sense, what distinguishes digital platforms' content selection practices from those of traditional media is the knowledge (i.e., data) and the technical tools (i.e., machine-learning algorithmic systems) for commanding online attention, which together grant platforms an unprecedented potential for persuasion.[11]
An attention economy based on surveillance capitalism presents multiple negative side effects for both individuals and society,[12] including addiction,[13] the amplification of extreme content,[14] and the formation of "echo chambers",[15] where users are primarily exposed to a highly tailored package of information designed to match their preexisting interests and beliefs.[16] Moreover, since recommender systems are designed to identify

[9] N. Helberger, *The Political Power of Platforms: How Current Attempts to Regulate Misinformation Amplify Opinion Power*, in *Digital Journalism,* 8(6), 2020, esp. 846.

[10] N. Helberger et al., *Choice Architectures in the Digital Economy: Towards a New Understanding of Digital Vulnerability*, in *Journal of Consumer Policy,* 45(2), 2022, esp. 176. This form of hyper-individualized computational advertising, based on the monitoring of online behaviour and depending on granular-level data collection, mining, aggregation, and ad serving, is generally referred to as "online behavioural advertising" (OBA), see: N. Helberger et al., *Macro and Exogenous Factors in Computational Advertising: Key Issues and New Research Directions*, in *Journal of Advertising,* 49(4), 2020, esp. 382.

[11] N. Helberger, *The Political Power of Platforms*, cit., esp. 846.

[12] J. Cohen, *Between Truth and Power*, cit., esp. 85.

[13] European Parliament, *New EU Rules Needed to Address Digital Addiction*, 12 December 2023; F. Esposito – T. M. C. Ferreira, *Addictive Design as an Unfair Commercial Practice: The Case of Hyper-Engaging Dark Patterns*, in *European Journal of Risk Regulation*, 15(4), 2024, 999 ff.

[14] D. Murthy, *Evaluating Platform Accountability: Terrorist Content on YouTube*, in *American Behavioral Scientist*, 65(6), 2021, 800 ff.

[15] E. Pariser, *Il Filtro,* cit.; C. R. Sunstein, #*Republic: Divided Democracy in the Age of Social Media*, NED-New edition, Princeton, 2018.

[16] T. Wu, *Is the First Amendment Obsolete?*, cit., esp. 555. The aspiration to give everyone their tailored news outlet has been also confirmed by Mark Zuckerberg himself, when stating that: «Our goal is to build the perfect personalized newspaper for every person in the world». See: M. Moore, *Tech Giants and Civic Power*, London, 2016, esp. 32. However, such mechanisms risk entrenching users' existing views, leading to a societal fragmentation. See: J. Habermas, *Nuovo mutamento della sfera pubblica e politica deliberativa*, Milan, 2023. Additional polarisation

and exploit user vulnerabilities to effectively target content,[17] and their functioning has been traditionally opaque,[18] they heighten the potential for manipulation,[19] significantly affecting individual capacity to make free choices and, ultimately, autonomy and self-determination.[20] These concerns are related to both "users-as-consumers", with respect to their ability to make rational choices on the market,[21] and to "users-as-citizens", concerning their access to plural information and the formation of their political opinions.[22] In this context, several values and rights of the European Union may be at risk, including individual autonomy and personal development as elements of the right to private life, the right to receive and impart information,[23] information pluralism, as well as competitive

would occur when extreme content is prioritised, meaning that «everyone sees exactly the information that personally aggravates them». See: A. Geese, *Why the DSA Could Save Us From the Rise of Authoritarian Regimes*, in *Putting the Digital Services Act into Practice*, ed. J. van Hoboken, Amsterdam, 2023, esp. 71. This self-reinforcing exposure dynamic, where recommender systems gradually lead users toward increasingly radical content is often referred to as the "rabbit hole" effect. See: K. Woolley - M. A. Sharif, *Down a Rabbit Hole: How Prior Media Consumption Shapes Subsequent Media Consumption*, in J*ournal of Marketing Research,* 59(3), 2022, 453 ff.

17 N. Helberger et al., *Choice Architectures in the Digital Economy,* cit.; P. Armstrong, *Facebook Is Helping Brands Target Teens Who Feel 'Worthless'*, in *Forbes*, accessed 11 September 2025.

18 F. Pasquale, *The Black Box Society: The Secret Algorithms That Control Money and Information*, Cambridge, 2015.

19 R. Calo, *Digital Market Manipulation*, in *George Washington Law Review*, 82, 2014, 995 ff.; N. Helberger et al., *Choice Architectures in the Digital Economy*, cit., esp. 186; J. Cohen, *Between Truth and Power*, cit., esp. 86.

20 E. Izyumenko et al., *Online Behavioural Advertising, Consumer Empowerment and Fair Competition*, cit., esp. 6; A. Bradford, *Digital Empires*, cit., esp. 8; D. Susser - B. Roessler - H. Nissenbaum, *Online Manipulation: Hidden Influences in a Digital World*, in *Georgetown Law Technology Review,* 4(1), 2019.

21 E. *Izyumenko et al., Online Behavioural Advertising, Consumer Empowerment and Fair Competition,* cit.*,* esp. 6*;* N. Helberger et al., *Choice Architectures in the Digital Economy,* cit.; N. Helberger et al*., Macro and Exogenous Factors in Computational Advertising*, cit., esp. 382. The concerns related to consumer protection are to be addressed in a forthcoming Digital Fairness Act: European Commission, *Commission Launches Open Consultation on the Forthcoming Digital Fairness Act | Shaping Europe's Digital Future*, European Commission | Digital Strategy, 17 July 2025.

22 J. Burkell - P. M. Regan, *Voter Preferences, Voter Manipulation, Voter Analytics: Policy Options for Less Surveillance and More Autonomy*, in *Internet Policy Review*, 8(4), 31 December 2019. The Cambridge Analytica scandal is a prime example in this regard: the company harvested personal data from millions of Facebook users without their consent and used it to build detailed individual profiles, which were then exploited to deliver highly personalised political advertising and allegedly influencing elections, including the 2016 U.S. presidential race and the Brexit referendum. See: M. Rosenberg - N. Confessore - C. Cadwalladr, *How Trump Consultants Exploited the Facebook Data of Millions*, in *The New York Times,* 17 March 2018.

23 E. Izyumenko et al., *Online Behavioural Advertising, Consumer Empowerment and Fair Competition*,

market dynamics and democratic processes.[24]

Against this background, recent EU regulations have introduced several provisions governing targeted online advertising and recommender systems, which broadly appear to foster users' autonomy in relation to content recommendations.[25] Since personalisation constitutes a main feature of recommender systems, rules on the protection of personal data, as primarily established by the General Data Protection Regulation (GDPR),[26] are central in this context. Building on the GDPR, more specific provisions have since been introduced by the Digital Services Act (DSA),[27] the Digital Markets Act (DMA),[28] and the Regulation on Transparency and Targeting of Political Advertising (PAR).[29] This work thus analyses these three key regulatory frameworks (respectively in Section 2, Section 3, and Section 4) in light of their effectiveness in protecting users' autonomy online, also assessing, where possible, their practical implementation.[30] The objective of this work is therefore to examine through which legal mechanisms the EU legislator has decided to protect users' autonomy in relation to algorithmic recommendations, to assess the potential weaknesses of these rules, and to identify the aspects that could be further strengthened. Since recommender systems are generally machine-learning algorithmic systems, the Artificial Intelligence Act (AI Act) is also, in principle, applicable to them.[31] However, this Regulation does not appear to have been

cit., esp. 9; B. Roessler, *The Value of Privacy*, Cambridge, 2005.

[24] E. Izyumenko et al., *Online Behavioural Advertising, Consumer Empowerment and Fair Competition*, cit., esp. 6.

[25] Importantly, the EU can regulate these technologies only insofar as needed for the protection and the development of the internal market, since 114 TFUE constitute the legal basis for these regulations. See: N. Helberger et al., *Choice Architectures in the Digital Economy*, cit., esp. 198.

[26] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

[27] 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).

[28] Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act).

[29] Regulation (EU) 2024/900 of the European Parliament and of the Council of 13 March 2024 on the transparency and targeting of political advertising.

[30] However, given the rapidly evolving nature of both the regulatory landscape and platform policies, these insights may soon become outdated.

[31] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June

primarily designed to govern content curation algorithms within online platforms. The transparency obligation imposed on providers of AI systems that interact directly with natural persons seems mainly relevant for chatbots,[32] while the provisions on systemic risk assessment add little when the provider is already designated as a VLOP or VLOSE under the DSA.[33] It should also be noted that the AI Act prohibits AI systems deploying «subliminal» techniques intended to «manipulate» a person's behaviour by «impairing their ability to make an informed decision» and thereby causing «significant harm»; as well as those exploiting «vulnerabilities» linked to age, disability or a social-economic situation with the objective of «distorting the behaviour of that person» and thereby causing «significant harm».[34] Given the manipulative potential of recommender systems, it is worth considering whether these prohibitions could apply in this context.[35] However, no official guidance or enforcement precedent has yet clarified this point.

The AI Act's lack of specific provisions on content recommendation is particularly problematic in light of the emerging role of generative AI systems in accessing information online.[36] While the European Commission

2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act), art. 3.

[32] AI Act, art. 50(1). art. 50(4) also requires AI systems deployers to disclose artificially generated content and *deepfakes*.

[33] AI Act, art. 55. VLOP and VLOSE are defined below, in Section 1.

[34] AI Act, art. 5(1), (a), (b). Some issues related to the interpretation of these provisions can be found in: F. Lupiáñez-Villanueva et al., *Behavioural Study on Unfair Commercial Practices in the Digital Environment: Dark Patterns and Manipulative Personalisation*, European Commission | Directorate-General for Justice and Consumers, 2022, esp. 83; European Commission, *Commission Staff Working Document | Fitness Check of EU Consumer Law on Digital Fairness*, SWD(2024) 230 final, 3 October 2024, esp. 167.

[35] The AI Act (recital 29) clarifies that advertising that complies with the applicable law should not be regarded as harmful or manipulative *per se*.

[36] The launch of ChatGPT may already have marked a turning point in the global structure of content transmission and accessibility, as models like ChatGPT are increasingly used as substitutes for search engines. Recently, Open AI also launched its own browser, ChatGPT Atlas, and an artificially generated social media, Sora. See: L. Eadicicco, *The Battle for the Future of the Internet Is Underway*, in *CNN*, 22 October 2025; L. Eadicicco, *The next Era of Social Media Is Coming. And It's Messy so Far*, in *CNN*, 11 October 2025. Moreover, traditional search engines such as Google begun integrating AI-generated summaries as the first result displayed to users' queries, generating significant complaints from news providers and certain content-providing platforms. See: The Economist, *AI Is Killing the Web. Can Anything Save It?*, in *The Economist*, 14 July 2025; A. Lieb - A. Chapekis, *Google Users Are Less Likely to Click on Links When an AI Summary Appears in the Results*, in *Pew Research Center*, 22 July 2025; F. Y. Chee, *Exclusive: Google's AI Overviews Hit by EU Antitrust Complaint from Independent Publishers*, in

seems aware of the need to extend certain rules on content selection practices on generative AI systems,[37] the application of existing frameworks faces significant obstacles. When generating their own outputs rather than merely providing access to third-party content, these technologies are unlikely to meet the definition of digital platforms, thereby falling outside the scope of the DSA.[38] Moreover, they do not currently appear among the core platform services listed under the DMA.[39] Conversely, the Regulation on Political Advertising, which is not limited to platform services, would apply to such providers if they were to offer advertising services.[40] Likewise, the GDPR remains fully applicable to their data processing activities.[41]

2. The DSA Regulating Recommender Systems

The Digital Services Act recognises, in its preamble, that the ranking of information is a fundamental aspect of platforms' activities and that it has a significant impact on users' ability to encounter information online, as well as contributing to the amplification of certain content.[42] In this regard, the DSA emphasises the need for users to be adequately informed about how recommender systems influence the reception of information. This means that one of the main purposes of the DSA regarding recommender systems is to address the information asymmetry traditionally existing between platforms and the public society in this context.[43] Beyond

Reuters, 4 July 2025; M. Miller, *New User Trends on Wikipedia,* in *Diff,* 17 October 2025.

[37] Euractiv, *Commission Checking If ChatGPT Falls under EU Online Governance Rules*, in *Euractiv*, 22 October 2025.

[38] The definition of digital platforms and the analysis of the scope of the DSA are further discussed below, in Section 1.

[39] However, the European Commission is empowered to enlarge the list of "core platform services" through delegated acts (DMA, Art. 12). The scope of the DMA is further discussed below, in Section 3.

[40] OpenAI has indeed started offering advertising services on ChatGPT: OpenAI, *Test degli annunci in ChatGPT*, in *Open AI*, 9 February 2026.

[41] While the AI Act remains largely silent on content selection, this aspect could arguably be addressed within its general provisions on systemic risk assessment (art. 55).

[42] DSA, recital 70.

[43] A. Geese, *Why the DSA Could Save Us From the Rise of Authoritarian Regimes*, cit., esp. 69. Some transparency requirements could already arguably be found in the GDPR with regards to automated data processing practices and, particularly, automated decision making. See: E. Izyumenko et al., *Online Behavioural Advertising, Consumer Empowerment and Fair Competition*, cit., esp. 15; N. Helberger et al., *Macro and Exogenous Factors in Computational Advertising,* cit., esp. 382; C. Panigutti et al., *The Role of Explainable AI in the Context of the AI Act*, in *Association for*

transparency, the DSA also seeks to limit the most high-risk recommender systems, thereby imposing several restrictions on targeted advertising and profiling practices. Following the system of escalating obligations characterising the DSA,[44] some of the provisions examined in this Section apply to intermediaries qualifying as online platforms,[45] while additional ones are imposed on platforms designated by the European Commission as Very Large Online Platforms (VLOPs) and Very Large Online Search Engines (VLOSEs).[46]

2.1. Transparency Obligations on Recommender Systems

The DSA includes a wide range of transparency obligations.[47] This Section first examines general transparency obligations for recommender systems and then addresses those specifically related to advertising.

2.1.1. General transparency obligations for recommender systems

The first transparency requirement concerning recommender systems is

Computing Machinery, FAccT '23, 12 June 2023, esp. 1141.

[44] A. Vicinanza, *La responsabilità delle piattaforme digitali nei confronti dei contenuti illegali: dal caso Telegram al Digital Services Act*, Quaderni AISDUE, 1/2025, 195 ff.

[45] As defined by the DSA, art. 1(i). Essentially, platforms are digital intermediaries that store information provided by a recipient, with the ability to make that information publicly available at the recipient's request. Accordingly, platforms are understood to possess two essential features: (1) the carriage of third-party content; (2) the potential public dissemination of that content.

[46] As defined by the DSA, art. 33(1). The designation by the European Commission follows a dimensional criterion based on the number of average monthly active users, which must, in principle, be equal or exceed 45 million. The DSA's preamble acknowledges that these large platforms play a major role in facilitating public debate, as well as in economic operations (recital 75), posing a public policy concern which justifies the imposition of additional obligations, including the need to address "systemic risks" stemming from their services (recital 79). As for now, 22 VLOPs and 2 VLOSEs have been designated (information can be found on the Commission's website: European Commission, *Supervision of the Designated Very Large Online Platforms and Search Engines under DSA*, in *Shaping Europe's Digital Future, European Commission*, accessed 21 March 2025.

[47] Other provisions include transparency on moderation practices (arts. 14 and 15), as well as external oversight obligations (e.g., the requirements for VLOPs and VLOSEs to undergo independent audits at least once a year in line with art. 37 DSA, and to provide vetted researchers with access to their data in line with art. 40 DSA).

established by art. 27 of the DSA, which obliges online platforms to explain in their terms and conditions «in plain and intelligible language» the main parameters used in their recommender systems. The purpose of this obligation is to enable users to understand why certain content is recommended to them.[48] This explanation must include the most important criteria used for content recommendation, with the indication of their respective importance.[49] Moreover, the platform must inform users about any option to "modify or influence" the main parameters used for recommendation, and provide an easily-accessible functionality to modify at any time the preferred option.[50]

Scholars have examined how Meta and TikTok have implemented art. 27 of the DSA.[51] Both companies have introduced explanations about the impact of user behaviour and interactions within the platform on the content recommended to them.[52] However, while the DSA mandates transparency on how user behaviour influences content recommendation, an obligation to provide users with options to modify the parameters used by recommender systems does not clearly result from the text, and platforms have followed a rather minimalistic interpretation of this provision, granting limited control to users over these systems.[53] Meta and TikTok only allow users to choose from a narrow list of reasons to indicate why they dislike a particular piece of content or specify hashtags they want to filter out of their feeds.[54] Additional control has been provided through the introduction of a "Refresh" option on TikTok, allowing users to reset their recommendations as if they were new to the platform;[55] representing however more of an all-or-nothing approach.

---

[48] DSA, art. 26(1).

[49] DSA, art. 26(2).

[50] DSA, art. 26(3). This functionality should be accessible on the interface where the information is prioritised.

[51] U. Reviglio – M. Fabbri, *The Regulation of Recommender Systems Under the DSA: A Transition from Default to Multiple and Dynamic Controls?*, in *DSA Observatory*, 22 November 2024.

[52] Meta, *Our Approach to Explaining Ranking*, in *Meta, Transparency Centre*, accessed 4 November 2025 ; TikTok, *How TikTok Recommends Content*, in *Tiktok.Com*, accessed 13 October 2025,

[53] U. Reviglio - M. Fabbri, *The Regulation of Recommender Systems Under the DSA*, cit., esp. 3. Conversely, codes of practices foresaw an obligation to grant users different options of recommender systems. See: European Commission, *2022 Strengthened Code of Practice on Disinformation | Shaping Europe's Digital Future*, in *European Commission*, accessed 7 October 2025.

[54] U. Reviglio – M. Fabbri, T*he Regulation of Recommender Systems Under the DSA*, cit., esp. 3.

[55] TikTok, *An Update on Fulfilling Our Commitments under the Digital Services Act*, in *Newsroom, TikTok*, 16 August 2019. This function has been recently added on Instagram as well: Instagram, *New on Instagram: How to Reset Your Content Suggestions*, in *Instagram*, 19 November 2024.

Conversely, wider control over recommendations would require not only filtering options to exclude certain content but also mechanisms to include it, allowing users to positively shape their results. Taking Instagram as an example, some minor options are available in this regard.[56] For instance, users can adjust the amount of sensitive[57] and political[58] content recommended to them, choosing between "Less", "Standard", and "More".[59] In addition, users are sometimes allowed to indicate whether they are interested in a specific piece of recommended content. However, the impact of the "Interested" option on recommendations remains unclear. More broadly, it seems like users on both platforms can only influence how content is displayed but cannot remove the original parameters that led to its recommendation. In other words, one can only modify the outputs, not the inputs. A different approach could provide users with the choice about which data feeds personalisation, e.g., their profile data or behavioural signals. This would also help users to understand the recommender system logic, allowing them to opt out of certain types of profiling that may not align with the user's actual or consciously expressed preferences.[60]

2.1.2. Transparency obligations for online advertisement

Art. 26 of the DSA introduces a series of transparency obligations regarding online advertising. First and foremost, commercial communications must be clearly labelled as such, ensuring a distinction between advertisement and other recommended content. Second, users must have access to information about the source of the advertisement and the reason it is recommended to them. Indeed, the preamble states that users must be informed about the main parameters used to determine why a specific advertisement is presented to them, including a «meaningful explanation of the logic» behind such recommendations, particularly when they rely on profiling.[61] Moreover, art. 39 strengthens advertising transparency for VLOPs and VLOSEs by requiring them to maintain a publicly accessible database containing key information about every advertisement displayed for a period of one year. The information to be disclosed includes the

[56] Broad information about content preferences can be found here: Instagram, *Control Your Instagram Feed*, in *Instagram Blog*, 30 August 2022.

[57] Instagram, *Updates to the Sensitive Content Control*, in *Instagram Blog*, 6 June 2022.

[58] Instagram, *Update on Political Content on Instagram and Threads*, Instagram, 9 February 2024.

[59] The "more" option is excluded for minors regarding sensitive content.

[60] U. Reviglio - M. Fabbri, *The Regulation of Recommender Systems Under the DSA*, cit., esp. 8.

[61] DSA, recital 68.

advertised product, the advertiser, the period during which the advertisement was displayed, the targeting parameters used, and the number of users reached.[62]

Regarding the actual implementation of advertising transparency, it is useful to examine how art. 26 has been operationalised on Instagram. In the Instagram feed, advertised content is labelled as "*Sponsored*". Users can access additional information directly from the advertised content by selecting the "Why you're seeing this ad" option (Figure 2).

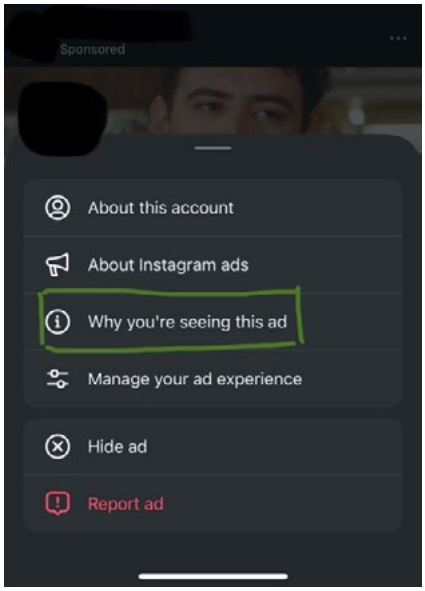

Figure 2. Instagram's options on each sponsored content, including "why you're seeing this ad" (screenshot taken on February 6, 2025)

This feature discloses the targeting parameters used for recommending the advertisement, which are divided into two categories (Figure 3),[63] namely

[62] DSA, art. 39(1). The legality of the obligation to make an advertisement repository publicly available has been contested by certain designated VLOPs. See: CJEU, Case T-367/23, *Amazon Services Europe v Commission*, action brought on 5 July 2023. Amazon essentially held that this provision infringes its fundamental rights to privacy and its freedom to conduct a business, essentially because it entails the disclosure of confidential information to competitors. While the Court has not yet ruled the substance of the case, it rejected Amazon's request for interim measures. Seee: Amazon Services Europe Sàrl v European Commission, Case T-367/23 R (Order of the President of the General Court of 27 September 2023, Court of Justice of the European Union). Indeed, the Court held that postponing the DSA's objective of enhancing transparency and accountability for major platforms could pose significant risks. Although not conclusive, this decision has been regarded as an indication that the Court is likely to attach significant weight to the public interest pursued by the DSA and to uphold its data-sharing and transparency provisions. See: B. Botero Arcila, *An Early Win for the Transparency Measures of the DSA. A Comment on Amazon Services v. European Commission (C-638/23)*, in *DSA Observatory*, 2 May 2024.

[63] They are divided into two categories only if the user has selected the "more personalised" version of the platform (see *infra*: Section 3). Otherwise, since ads are not based on profiling,

advertiser choices about the demographics that they want to target and user activity.

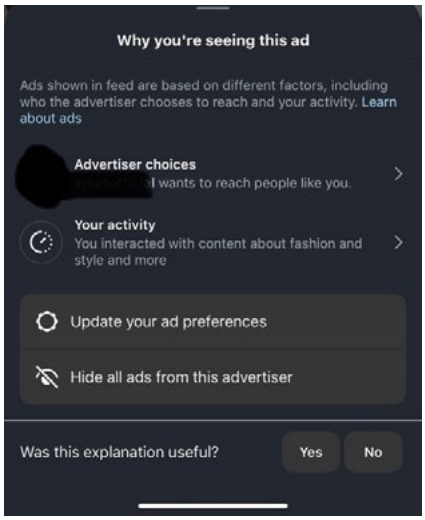

Figure 3. Explanation on "why you're seeing this ad" on Instagram: advertisers' choices and individual users' activity (screenshot taken on February 6, 2025)

Therefore, the first category includes parameters selected by the advertiser, who may choose to target users based on factors such as "an age between 18 and 45", "a primary location in Italy", or gender (Figure 4).[64]

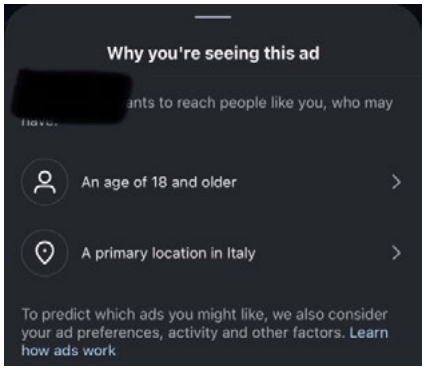

Figure 4. Explanation on "why you're seeing this ad" on Instagram: the criteria selected by the advertiser to target the user (screenshot taken on February 6, 2025).

The second category includes parameters linked to the individual user's activity, reflecting personalised advertising based on profiling techniques.[65] In this case, the advertisement is deemed relevant to the targeted user based on inferences drawn from previous interactions on the platform or on other services. For example, in the case of an advertisement from a fashion company, this category included parameters such as "you interact-

only the first category appears.

[64] These are the only targeting criteria for users who selected the less personalized version with ad breaks (see *infra*: Section 3).

[65] This category of targeting criteria only concerns users who selected the more personalized version of the service without ad breaks.

ed with ads about fashion and style, clothing and travel", but also "about pets, relationships and software and apps", including interactions on Facebook Marketplace (Figure 5).

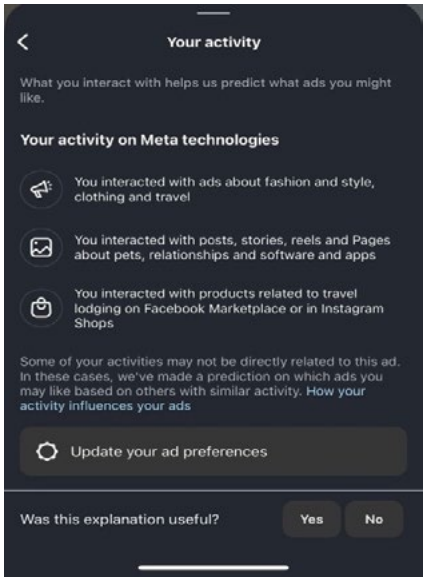

Figure 5. Explanation on "why you're seeing this ad?" on Instagram based on the user's activity (screenshot taken on February 6, 2025).

When examining the operationalisation of these transparency requirements, the overall picture appears rather unsatisfactory. Indeed, the displayed explanations appear confusing and fail to provide any meaningful insight. Not only are the mentioned parameters exceedingly broad, but the lack of reference to specific actions makes it unclear how these interests are determined, while the connection between certain topics – such as pets and fashion – is not immediately evident. Ultimately, this information does not enable users to answer the "Why me?" question.[66]

When accessing this feature, users can also access Instagram's parent company (Meta) advertisement database, where they can view all ads from the same source over the past year, even if they are no longer active. By clicking on an individual advertisement, users can see who paid for it and on whose behalf, as well as the approximate number of impressions it received. Additionally, the Meta advertisement database can be accessed directly via the web and includes ads across all Meta platforms. The database is accessible through a search function with filters by country and theme, including issues, elections, or politics; housing; employment; finan-

[66] E. Izyumenko et al., *Online Behavioural Advertising, Consumer Empowerment and Fair Competition*, cit., esp. 14. It must be observed that making algorithms and AI systems explainable constitutes a significant technological challenge: N. Helberger et al., *Macro and Exogenous Factors in Computational Advertising*, cit., esp. 385; C. Panigutti et al., *The Role of Explainable AI in the Context of the AI Act,* cit.

cial products and services.[67]
Other than imposing obligations on the transparency of recommender systems, the DSA also imposes some substantial limitations on targeting practices, especially when performed through profiling activities.

2.2. Restrictions on Targeted Recommendations

As mentioned in the introduction of this Section, the DSA also addresses certain content microtargeting practices. These provisions are largely based on the GDPR, including several references to its rules and definitions.

2.2.1. Restrictions on profiling practices for online advertising

The DSA includes two prohibitions concerning targeted advertising: the first, outlined in art. 26, focuses on "sensitive" data, while the second, art. 28, concerns advertising targeting minorsArt. 26, in its final paragraph, prohibits online platforms from presenting advertisements to users based on profiling using the special categories of data defined by art. 9 of the GDPR. Profiling, as defined by the GDPR,[68] is an automated process involving the use of a set of personal data about an individual or a group of people to generate new insights, meaning inferred knowledge or hypotheses about a person's behaviour, such as their preferences, personality, or health conditions.[69] The prohibition outlined by art. 26 refers to particularly sensitive data identified by the GDPR, such as those related to ethnic origins, political opinions, religion, or sexual orientation.[70] Under the

[67] These findings are based on research conducted on Meta platforms by the author on February 6, 2025, but the situation may evolve rapidly. For advertisements categorized under "Issues, elections, or politics" users can immediately see the estimated audience size and the approximate amount spent, and it is possible to rank results based on the number of impressions received This additional information are connected to the requirements set by the Regulation on Political Advertisement, as further discussed below (Section 4).

[68] GDPR, art. 4(4), defines profiling as «any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements».

[69] L. Edwards – M. Veale, *Slave to the Algorithm? Why a "Right to an Explanation" Is Probably Not the Remedy You Are Looking For*, in *Duke Law & Technology Review,* 16(1), 2017, esp. 32.

[70] GDPR, art. 9: special categories of data are those «revealing racial or ethnic origin, political

GDPR, processing this data is prohibited, with however some significant exceptions, including the existence of an explicit and specific consent of the data subject. In contrast, under the DSA, profiling using such personal data for targeted advertising is entirely prohibited, without exception.

The decision to entirely prohibit the targeting of advertising based on profiling involving particularly sensitive data, regardless of user consent, represents a highly reasonable approach on multiple levels, particularly in light of the often fictitious nature of consent in the digital environment.[71] Moreover, by acknowledging that targeting users with advertisements tailored to their interests and potentially exploiting their vulnerabilities can have serious negative effects, the DSA addresses not only individual but also societal harms. Manipulative techniques can damage entire groups and amplify collective risks, for example, by fuelling disinformation campaigns or enabling discriminatory practices.[72] Unlike the GDPR, which primarily focuses on the protection of individual rights and therefore relies on consent, this provision appropriately considers data protection as a tool to safeguard society as a whole from manipulation.[73]

However, these provisions also present some weaknesses. First, not all data that may be regarded as sensitive when used for commercial purposes (for example, information about mental states or financial difficulties) is included in art. 9 of the GDPR.[74] Second, manipulation is not only possible using particularly sensitive data but can also be carried out by exploiting large-scale, detailed datasets. Indeed, vulnerability is not solely connected to the use of special categories of data, but to the functioning of targeting practices *per se*.[75] Indeed, this provision represents more of a compromise between a total ban on personal data for targeting advertising (as mandated by art. 28 for minors) and the previous situation, where any

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».

[71] L. Edwards – M. Veale, *Slave to the Algorithm?*, cit., esp. 33; Cohen, *Between Truth and Power*, cit., esp. 44. This issue was also addressed by the Court of Justice stating in *Meta platforms* (n 80) that "consent" to certain data processing practices on Facebook could not be considered as freely given since it was a precondition for accessing Facebook's services, and Facebook's dominant market position left users with no real alternatives (see *infra*).

[72] DSA, recital 69.

[73] A. Geese, *Why the DSA Could Save Us From the Rise of Authoritarian Regimes,* cit., esp. 71.

[74] Such issue has been acknowledged by the European Commission when assessing the adequacy of consumer protection in the current digital environment, see: European Commission, *Commission Staff Working Document | Fitness Check of EU Consumer Law on Digital Fairness,* cit.*,* esp. 166.

[75] N. Helberger et al., C*hoice Architectures in the Digital Economy*, cit., esp. 190.

data processing was permitted insofar as it was in line with the GDPR.[76]
Third, platforms and advertisers may be tempted to bypass legal restrictions on the use of sensitive data by relying on so-called "proxy" variables, i.e., seemingly neutral data points that can nonetheless serve as indicators of sensitive attributes. For example, a person's location history, online activity, or purchasing habits may indirectly reveal sensitive characteristics such as their political views, religious beliefs, or health conditions. This issue is connected to the regulation of profiling techniques inferring sensitive information from data that are not, in themselves, sensitive.[77] However, the preamble of the DSA seems to include this type of profiling within the scope of the prohibition.[78]
Finally, distinguishing sensitive data within vast datasets can prove challenging. Internal Facebook documents leaked through Frances Haugen's whistleblowing activity revealed that the company struggled to identify the different types of data it was storing and using.[79] In any case, the Court of Justice of the European Union ruled that when data is processed collectively *en bloc* and it is not possible to distinguish among different categories, all such data should be treated under art. 9 of the GDPR.[80] If applied more broadly, this principle implies that, whenever such a distinction cannot be made, a higher standard of protection should apply, including in the context of DSA's implementation.
As for art. 28 of the DSA, it begins with a general obligation for online platform providers to adopt appropriate and proportionate measures to ensure a high level of privacy, safety, and security of minors using their services. The second part of the article prohibits platforms from targeting online advertising based on profiling when they are aware with reasonable certainty that the recipient of the service is a minor. At the same time, it explicitly states that platforms are not required to collect additional personal data to determine whether a user is a minor. Unlike art. 26, in this case, profiling for advertisement purposes is entirely prohibited, regardless of the type of data used. However, since only profiling is restricted, it

[76] A. Geese, *Why the DSA Could Save Us From the Rise of Authoritarian Regimes*, cit., esp. 70.

[77] L. Edwards – M. Veale, *Slave to the Algorithm?*, cit., esp. 37.

[78] DSA, recital 69: «[…] providers of online platforms should not present advertisements based on profiling […], using special categories of personal data […], including by using profiling categories based on those special categories».

[79] According to one of the leaked documents, a Facebook engineer stated: «We do not have an adequate level of control and explainability over how our systems use data, and thus we can't confidently make controlled policy changes or external commitments such as "we will not use X data for Y purpose". And yet, this is exactly what regulators expect us to do». See*:* L. Franceschi-Bicchierai, *Facebook Doesn't Know What It Does With Your Data, Or Where It Goes: Leaked Document*, in *VICE*, 26 April 2022.

[80] CJEU, *Meta platforms and Others* (n 80), esp. §89.

appears that contextual targeting remains possible. This raises a broader issue, as the provisions analysed concern only profiling-based advertising, potentially leaving contextual advertising based on sensitive data, including the user's status as a minor, outside the scope of the DSA's prohibitions.

2.2.2. Right to access an option of recommender systems not based on profiling

In addition to this, art. 38 of the DSA requires VLOPs and VLOSEs to offer at least one option of their services where recommender systems are not based on profiling. Despite the conciseness of this provision, it represents one of the most significant rules concerning recommender systems since granting users access to an unfiltered version of information can enhance awareness of how algorithms shape information transmission and decrease the risk of manipulation. At the same time, this requirement strikes at the core of platforms' business model, as described above, because it undermines their ability to monetise user engagement. For this reason, this provision has been strongly criticised by Big Tech, which argued that non-personalised recommendations would reduce customers' satisfaction and weaken their competitiveness.[81]
When examining the current implementation of this rule, its impact does not appear, however, to be particularly disruptive. Using Instagram as an example, in order to comply with this requirement, since March 2022, users have been able to switch their feed display from the default "For you" option to the "Following" option.[82] When selecting the latter, the content displayed consists solely of material from accounts the user follows, shown in chronological order.[83] Although this feature may enhance the understanding of the content users encounter, or do not encounter, due to algorithmic filtering, it remains unclear how many users actually make use of this option or are even aware of its existence. Moreover, a complete lack of personalisation may fail to meet users' needs for a certain degree

[81] A. Guzik – L. Weigl, *In Brussels We Trust? Preliminary Insights Into the Legal Challenges to the DMA and DSA*, in *Tech Policy Press*, 5 November 2024. In particular, Amazon, in the proceeding initiated to annul its designation as VLOP, argued that this provision would «alter one of the fundamental pieces of software underpinning its business», thereby causing a significant competitive disadvantage compared with online marketplaces that are not designated as VLOP. See: *Amazon Services Europe Sàrl v European Commission*, esp. §§ 29-40.

[82] Information can be found here: A. Mosseri, *Control Your Instagram Feed with Favorites and Following*, in *Instagram Blog*, accessed 7 February 2025.

[83] The same option is also available on TikTok: U. *Reviglio - M. Fabbri, The Regulation of Recommender Systems Under the DSA*, cit.

of content organisation,[84] limiting the practical usefulness of this option.[85] Conversely, providing users with the possibility to use, for instance, a recommender system that combines personalised and non-personalised content could prove more appealing.[86]

After outlining the restrictions on profiling imposed by the DSA, the next paragraph is dedicated to the rules on systemic risk assessment. The provisions analysed so far illustrate how the EU has identified and addressed what it considers the most significant risks related to recommender systems through a top-down approach. However, the DSA also requires major platforms to take an active role in identifying and mitigating additional risks that may emerge from the services they provide.

2.3. Systemic Risks Assessment on Recommender Systems

Platforms designated as VLOPs and VLOSEs are required under the DSA to assess and mitigate the systemic risks arising from their recommender systems, including their influence on the spread of illegal content and their potential impact on human rights, human dignity, democracy, civic debate, and electoral processes.[87] In addition to algorithms and recommender systems, platforms must also assess risks related to advertising and data processing, which are closely interconnected.

Under this framework, platforms should evaluate risks stemming from both the design of their algorithmic systems and their potential abuse by malicious actors. Regarding design, platforms are required to assess whether certain features inherently generate harmful consequences. This could be the case for algorithms primarily designed to maximise engagement, which may, for this reason, promote extreme content or create "rabbit hole" effects, as discussed above. Regarding abuse by malicious actors, platforms must assess whether their algorithmic systems contain vulnerabilities that could be exploited by third parties to generate undesirable effects on individuals or society.

The requirement to assess design-related risks is crucial, as it directly challenges platforms' business models, compelling them to evaluate their

[84] E. Izyumenko et al., *Online Behavioural Advertising, Consumer Empowerment and Fair Competition*, cit., esp. 23.

[85] U. Reviglio – M. Fabbri, *The Regulation of Recommender Systems Under the DSA,* cit.

[86] E. Izyumenko et al., *Online Behavioural Advertising, Consumer Empowerment and Fair Competition*, cit., esp. 24.

[87] DSA, art. 34 and 35.

potential negative impacts.[88] This is also linked to the issue of design liability, meaning that while platforms cannot be held liable for third-party content,[89] they can still be held accountable for their conduct, i.e., the way they choose to design their products. However, examining the first risk assessment reports publicly available,[90] some scholars noted that they primarily focused on harmful behaviour and abuse, largely omitting how the platform's design itself intersects with the main risks.[91]

The European Commission has issued several requests for information under the DSA specifically concerning recommender systems.[92] For instance, it requested YouTube and Snapchat to provide detailed information on the role of their algorithms in amplifying risks related to, *inter alia*, civic discourse and users' mental well-being, including addictive behaviour and content "rabbit holes". Addictive design is one of the central issues related to recommender systems,[93] and was the object of an opening of proceedings against TikTok and particularly its "Task and Reward Program".[94]

In any case, these issues are still evolving: the Commission's actions have initiated a broader dialogue, from which new mitigation measures may eventually emerge. Moreover, recommender systems and profiling practices are not only regulated by the DSA, but they are also addressed by other regulations, as examined below.

---

88 A. Geese, *Why the DSA Could Save Us From the Rise of Authoritarian Regimes*, cit., esp. 69.

89 For a discussion on platforms' liability framework, see: A. Vicinanza, *La responsabilità delle piattaforme digitali nei confronti dei contenuti illegali,* cit.

90 For some considerations on the first risk assessment reports, see: J. Albert, *DSA Risk Assessment Reports: A Guide to the First Rollout and What's Next*, in *DSA Observatory*, 9 December 2024. It must be noted that the publicly available version may differ from the one transmitted to the European Commission, as the publication is made on a voluntary basis.

91 P. Chapman, *Advancing Platform Accountability: The Promise and Perils of DSA Risk Assessments*, in *Tech Policy Press*, 9 January 2025. According someone this is particularly true for Meta's platforms, and less for others such as YouTube. See: T. Bernard, *Reading the Systemic Risk Assessments for Major Speech Platforms: Notes and Observations*, in *Tech Policy Press*, 20 December 2024.

92 European Commission, *Commission Sends Requests for Information to YouTube, Snapchat, and TikTok on Recommender Systems under the Digital Services Act*, in *European Commission*, Press Release, 2 October 2024.

93 P. Chapman, *Advancing Platform Accountability,* cit.

94 European Commission, *Commission Opens Proceedings against TikTok under the DSA*, in *European Commission*, 22 April 2024.

3. The DMA's Restrictions on the Use of Data and Their Impact on Recommender Systems

The Digital Markets Act has introduced certain restrictions on the use of personal data by platform service providers designated by the European Commission as "gatekeepers".[95] The main objective of the DMA is to ensure fair and contestable digital markets, primarily by limiting abusive practices by dominant online platforms.[96] The inclusion of data-related provisions is therefore unsurprising when considering that data constitute a critical asset for competition in digital markets.[97]

Art. 5(2) of the DMA restricts several combinations of user data, unless users are presented with a specific choice in this regard and subsequently give their consent in accordance with the GDPR.[98] The first limitation concerns the use of data for advertising purposes and applies to data collected from third-party services that are available on the gatekeeper's

[95] The designation as "gatekeeper" serves a similar purpose to that of VLOPs and VLOSEs under the DSA, as both classifications rely on platform size for imposing special obligations to the companies often referred to as "Big Tech" or "GAFAM". In both cases, designation is made by the European Commission, but while the VLOPs and VLOSEs' classification relies solely on a threshold of 45 million average monthly active users, the DMA requires additional criteria for presuming a gatekeeper position, including a threshold of yearly active *business* users on the platform service (at least 10,000); and an annual EU turnover of at least 7,5 billion euros over the last three years, or a market capitalisation of at least 75 billion euros in the previous financial year (DMA, art. 3). Under the DMA it is the undertaking providing the platform service that is designated as a gatekeeper, even though the designation applies specifically to one or more of its "core platform services" (DMA, art. 2). As of now, seven undertakings have been designated as gatekeepers, covering 24 platform services. See the European Commission official website: European Commission, *DMA Designated Gatekeepers*, in *European Commission*, accessed 13 October 2025. As a result, many gatekeepers also qualify as VLOPs and VLOSEs, including social networks (LinkedIn, Facebook, Instagram, TikTok), some intermediators (Amazon Marketplace, Google Shopping, Google Play, App Store, Google Maps, Booking.com), video-sharing platforms (YouTube), and search engines (Google Search). However, some platform services qualify as gatekeepers under the DMA but are not considered online platforms under the DSA, such as operating systems (Google Android, iOS, iPad iOS, Windows PC OS), personal communications services (WhatsApp, Messenger), browsers (Google Chrome, Safari), and advertisers (Google, Amazon, Meta).

[96] This goal is shared with traditional antitrust law, which, however, has faced certain shortcomings in the current digital ecosystem that have hindered its effectiveness, see: P. Manzini, *Il Digital Market Act Decodificato*, in *Unione Europea 2020 - I Dodici Mesi Che Hanno Segnato l'integrazione Europea*, Milan, 2021, esp. 324. In this context, the main contributions of the DMA compared to conventional antitrust law lies in the *ex ante* designation of dominant actors under the label of *gatekeepers*, accompanied by a detailed list of prohibitions and obligations.

[97] *Ibid.,* esp. *321*. Indeed, cases of data misuse have already been subject to antitrust litigation, as exemplified by the *Meta platforms* case (n 80).

[98] GDPR, art. 4(11) and art. 7.

platform.[99] This is coupled with a general restriction for combining data coming from third-party services[100] and from different services of the same company (e.g., Facebook and Instagram).[101] It is also specified that the gatekeeper must avoid signing in users to other platform services to combine personal data.[102] These provisions follow the purpose to limit the gatekeeper's privileged position on the market connected to its capacity to accumulate and monetise personal data coming from a wide set of services, thereby raising barriers to entry in the market.[103] However, the same provisions affect the functioning of recommender systems, which have traditionally relied on the combination of data from all possible sources, allowing for the creation of detailed user profiles.

The combinations of personal data described by art. 5(2) of the DMA are restricted but not prohibited, since the gatekeeper can lawfully perform them if it obtains users' specific consent or demonstrates another legitimate basis under the GDPR. Regarding alternative legitimate bases beyond consent, the DMA explicitly references only certain grounds established by the GDPR, including compliance with a legal obligation, protection of a person's vital interest, or performance of tasks carried out in the public interest.[104]

For defining consent, the DMA primarily refers to art. 4(11) of the GDPR, which defines it as a freely given, specific, informed, and unambiguous indication of will, as well as art. 7, which sets out the conditions for a valid consent. Additional details on the nature of user consent can be found in the DMA's preamble, which states that gatekeepers must allow users to freely opt-in to such data processing and sign-in practices by offering a «less personalised but equivalent *alternative*»,[105] meaning that the use of the core platform service or its functionalities must not be conditional on user consent. To meet this requirement, the less personalised alternative must «not be different or of degraded quality» compared to the service provided to users who have given consent, except where the degradation is a "direct consequence" of the gatekeeper's inability to process such

[99] DMA, art. 5(2), a).

[100] DMA, art. 5(2), c).

[101] DMA, art. 5(2), b) and c).

[102] DMA, art. 5(2), d).

[103] DMA, recital 36.

[104] More precisely, it references letters *(c)*, *(d)*, and *(e)* of art. 6(1) of the GDPR; while omitting *(b)* and *(f)*. This means the execution of contractual obligations and the legitimate interest of the processor do not qualify as valid grounds for the data processing-practices mentioned in art. 5(2) of the DMA. See also: DMA, recital 36.

[105] DMA, recital 36.

personal data.[106] From this, it follows that the essence of consent under the DMA lies in the ability to use platform services without being forced to agree to certain data processing practices.

These considerations around consent and the combination of user data largely echo a case before the German national competition authority regarding Meta platforms, which was later addressed by the Court of Justice of the European Union (CJEU).[107] The case originated from a proceeding by the *Bundeskartellamt* concerning Meta's practice of combining data collected on Facebook with "off-Facebook" data; specifically, data from its other services, such as Instagram, WhatsApp, and Oculus, as well as from third parties' websites. The Bundeskartellamt found that this practice violated both the GDPR and competition law, particularly as it represented an abuse of dominant position. According to the Bundeskartellamt, Meta's data processing practices lacked valid consent because users had no actual choice: consent was a precondition for accessing Facebook's services, and Facebook's dominant market position left users with no real alternatives.[108] On this point, the CJEU ruled that dominance *per se* does not invalidate consent under the GDPR. However, for the consent to be valid, users must be free to refuse data processing practices that are not necessary for the performance of the contract and must still be allowed to access an equivalent service, potentially for an appropriate fee.[109]

The data processing practices at issue in the *Meta* case substantially overlap with those addressed by art. 5(2) of the DMA. The notions of consent and the availability of alternative equivalent options for accessing services are also shared.[110] One notable difference, however, is that the CJEU judgement contemplated the possibility of charging a fee for accessing

[106] DMA, recital 37.

[107] Meta Platforms and Others, C-252/21 (Court of Justice of the European Union 2023). For a detailed analysis of all the questions addressed by the CJEU in this case, see: P. Manzini, *Antitrust e Privacy: La Strana Coppia*, in *I Confini Dell'antitrust. Diseguaglianze Sociali, Diritti Individuali, Concorrenza*, ed. Pietro Manzini, Turin, 2023, 123 ff.

[108] A. D'Amico et al., *Meta's Pay-or-Okay Model: An Analysis under EU Data Protection, Consumer and Competition Law*, in *Technology and Regulation,* 2024, 254 ff.

[109] CJEU, *Meta platforms* (n 80), §150. Beyond the issue of consent, the CJEU also examined other possible legal basis for data processing under the GDPR, substantially ruling out that these practices could be justified as necessary for the execution of the contract, or because falling within a legitimate interest of the platform (§97-124). The EDPB also found that Meta could not rely on reasons related to the execution of contract and legitimate interests for behavioural advertising purposes: European Data Protection Board, *Urgent Binding Decision 01/2023 Requested by the Norwegian SA for the Ordering of Final Measures Regarding Meta Platforms Ireland Ltd (Art. 66(2) GDPR),* European Data Protection Board, 7 December 2023.

[110] Moreover, the CJEU's exclusion of letters *(b)* and *(f)* of art. 6(1) GDPR as valid grounds for such data processing practices is likewise aligned with the DMA's provisions.

services without data combination, whereas the DMA remains silent on this point. This divergence created uncertainty as to whether Meta's subsequent "pay-or-consent" model, introduced in response to these regulatory developments, was compatible with the DMA's requirements.[111]

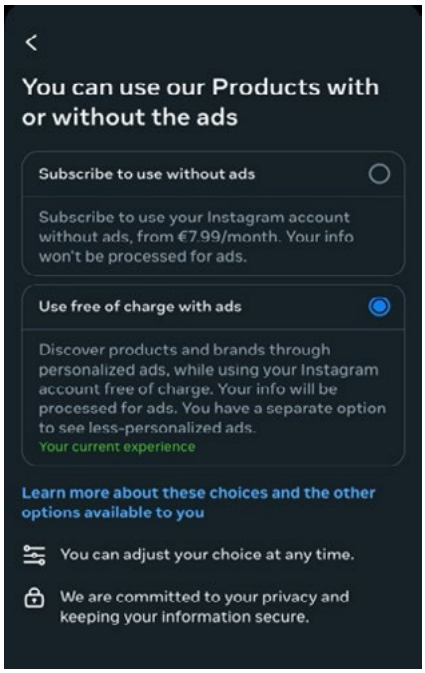

Figure 6. Pay or consent options (screenshot taken on Instagram on February 13, 2025)

To comply with the DMA, in November 2023, Meta sent to EU users of Facebook and Instagram a notification inviting them to choose between: (i) paying a monthly subscription for an ad-free experience, or (ii) continuing to access the platforms free of charge, agreeing to personalised advertising (Figure 6).[112] As a result, users were offered a new possibility to access Meta's services without consenting to the data processing covered by the DMA, although only by paying a fee of approximately €250 per year.[113] This system sparked renewed debates about users' freedom of choice, largely driven by civil-society organisations.[114] For instance, Noyb, a pri-

[111] Meta was among the first companies designated as gatekeeper by the European Commission, covering six core platform services: Facebook, Instagram, WhatsApp, Messenger, Meta Marketplace, and Meta Advertising. See: European Commission, *Digital Markets Act: Commission designates six gatekeepers,* European Commission, 6 September 2023, Press Release.

[112] Also referred to as "pay-or-okay" model.

[113] Noyb, *Statement on EDPB 'Pay or Okay' Opinion*, in *Noyb*, 17 April 2024. This fee was the lowered one year after (see *infra*).

[114] Noyb, *28 NGOs Urge EU DPAs to Reject "Pay or Okay" on Meta*, in *Noyb*, 16 February 2024. Similar considerations can be found here: Corporate Europe Observatory, *How Corporate Lobbying Undermined the EU's Push to Ban Surveillance Ads*, *Corporate Europe Observatory*, 18

vacy-focused NGO, highlighted that, although surveys indicated that only 3-10% of users wanted their personal data to be used for targeted advertising, 99% opted for the free version of Meta's services,[115] an outcome indicating a significant constraint on the genuine voluntariness of consent. The "pay-or-consent" model also came under the scrutiny of the European Commission,[116] which ultimately imposed a €200 million fine on Meta for the period during which "pay-or-consent" was the sole available option.[117]

However, the opening of proceedings by the Commission and the publication of its preliminary findings had already prompted Meta to revise its policies.[118] In November 2024, the company not only reduced the fee required to access the ad-free version (now amounting to approximately €95 per year) but also introduced an additional option allowing users to continue using the free version with a reduced collection of personal data for advertising purposes.[119] The free version now enables users to choose between a social media experience with advertisements that are either

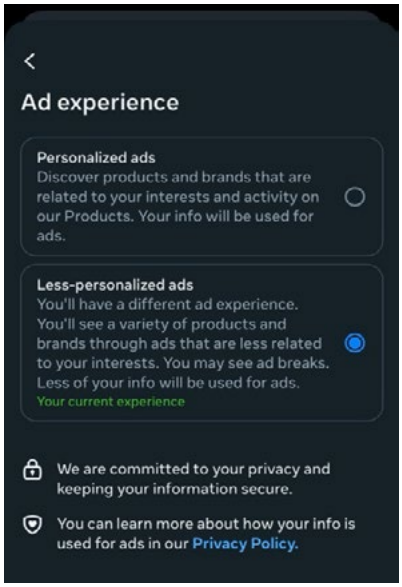

Figure 7. Different options for personalized advertisements on Instagram (screenshot taken on February 6, 2025)

January 2022.

[115] Noyb, *Statement on EDPB "Pay or Okay" Opinion,* cit..

[116] European Commission, *Commission opens non-compliance investigations against Alphabet, Apple and Meta under the Digital Markets Act,* European Commission, Press Release, 25 March 2024.

[117] European Commission, *Commission finds Apple and Meta in breach of the Digital Markets Act*, Press Release, European Commission, 23 April 2025.

[118] European Commission, *Commission sends preliminary findings to Meta over its "Pay or Consent" model for breach of the Digital Markets Act,* Press Release, European Commission, 1 July 2024.

[119] Meta, *Facebook and Instagram to Offer Subscription for No Ads in Europe*, in *Meta*, 12 November 2024.

"more" or "less" personalised (Figure 7). However, Meta has designed a less smooth browsing experience for users who refuse profiling-based ads, since they may now encounter unskippable "ad-breaks" lasting several seconds while using Meta's platforms, significantly slowing down navigation. Choosing the less personalised version with ad-breaks implies that advertisements are displayed solely based on contextual data, namely what a user views during a particular session on Facebook and Instagram, together with a minimal set of data points such as age, location, gender, and ad engagement.[120] This new option significantly alters the traditional functioning of recommender systems and, particularly, the degree of their personalisation. The transparency obligations on advertising imposed by the DSA make it possible to compare the targeting criteria applied to users who select the more personalised option with those who opt for the less personalised one.[121] A simple experiment analysing the advertisements shown to users under different settings indicates that users opting for the less personalised version (with ad-breaks) receive ads based only on basic criteria such as location, age, and gender (Section 1.1, Figure 4). In contrast, users opting for the personalised version are targeted through profiling, which relies on data about previous activity across different platforms, as well as interactions with other ads and users (Section 1.1, Figure 5). However, as previously observed, despite this additional information, understanding how profiling-based advertising operates remains difficult due to the vagueness of the descriptions provided.[122]

While the *ad-break* option could represent a better compromise for users compared to the paying option, its slower functioning could represent a significant disadvantage for those who use online platforms intensively, such as influencers, potentially discouraging them from opting out of profiling.[123] Comparing the new "ad-break" option with the "pay-or-consent" model, it appears that in both cases the reduced possibility to monetise user data is accompanied by a deliberate downgrading of the user experience by the platform provider. Although the options offered by Meta's platforms mostly emphasise content "personalisation", framed as a service provided in the users' interest, data collection primarily benefits the platform, representing its main source of revenue.[124] From this perspec-

[120] B. O'Donovan, *'Unskippable' Ads to Feature on Facebook and Instagram*, in *Raidió Teilifís Éireann (Rte)*, 12 November 2024.

[121] DSA, art. 27. See *supra* Section 2.1.

[122] See *supra*.

[123] At the same time, they could reduce user engagement, and becoming detrimental also for the platform itself (maybe this is the reason why, based on the author's personal experience) ad-breaks are increasingly rare on the platform (26 October 2025).

[124] S. Zuboff, *Il capitalismo della sorveglianza*, cit., 113.

tive, additional advertisements and subscription fees are presented as a form of compensation for the loss of revenue resulting from the reduced ability to monetise user data, once again highlighting the misleading nature of Facebook's former slogan, «It's free and always will be», which appeared on its login page until 2019.[125]
While the DSA and DMA provisions analysed in these first two Sections apply to all forms of advertising and recommender systems, even if some rules concern only certain categories of platforms, additional requirements have been introduced for political advertising through Regulation 2024/900, as examined below.

4. The Regulation on Political Advertising

Political advertising has always represented a democratic concern and has traditionally been regulated to ensure fair and transparent political processes.[126] On platforms, political advertising is mainly disseminated through recommender systems. The rise of targeted political advertising has raised new concerns, as massive data collection enables micro-targeting based on personal preferences and vulnerabilities, thereby amplifying the potential for manipulation, as exemplified by the Cambridge Analytica scandal.[127] In this context, the European Union adopted the Regulation on the Transparency and Targeting of Political Advertisement on 13 March 2024, whose main provisions are set to enter into force in autumn 2025.[128] The goal of this Regulation is to enhance the transparency of political advertising, enabling citizens to make informed decisions, preventing manipulation, and ensuring an open and free electoral process.[129] Addition-

[125] Q. Moynihan – A. Asenjo, *Facebook Quietly Ditched the 'It's Free and Always Will Be' Slogan from Its Homepage*, in *Business Insider*, 27 August 2019; M. Pennisi, *Facebook, perché sulla homepage non c'è più scritto «è gratis»*, in *Corriere della Sera*, 28 August 2019. Following regulatory scrutiny, Meta was then required to remove this slogan and to clarify in its terms of service that: «we don't charge you money to use our products because businesses and organizations pay us to show you ads». See: *A. Benckert, We're Updating Our Terms of Service to Better Explain How Facebook Works*, in *Meta*, 27 June 2019.

[126] D. Tambini, *Social Media Power and Election Legitimacy*, in *Digital Dominance. The Power of Google, Amazon, Facebook, and Apple*, by Damian Tambini and Martin Moore, Oxford, 2018, esp. 266.

[127] See *supra*.

[128] PAR, art. 30(2).

[129] PAR, recital 4. Among the general provisions now applicable to political advertising within the EU, it is worth mentioning the one preventing external interference in electoral processes. Indeed, art. 5(2) mandates that, during the three months preceding any voting process in the EU, providers of political advertisement services must only offer services to

ally, the Regulation introduces specific rules addressing online targeting techniques, which are considered a particular threat to fairness, transparency, and fundamental rights, including privacy and the right to receive proper information.[130] In this regard, the preamble highlights the growing frequency of tailored political content that leverages both observed and inferred personal data revealing political opinions, and is disseminated through often opaque algorithms.[131]

The Regulation applies to "political advertisement", which is defined as the «preparation, placement, promotion, publication, delivery or dissemination», by any means, of a political message. It specifies that such activities are typically provided behind remuneration, through in-house activities, or as part of a political advertising campaign. Moreover, for a message to qualify as political advertisement, it must either: *(i)* be provided by, for or on behalf of a political actor; or *(ii)* be suitable and designed to influence the outcome of a democratic process, including an election or referendum, voting behaviour or a legislative or regulatory process, at Union, national, regional or local level. The same article also specifies the definition of "political actor", which essentially refers to institutional political actors, such as parties, candidates, and members of public institutions.[132] Regarding geographical scope, the PAR applies when the political

an EU citizen, a permanent resident of a Member State, or a legal entity which is not owned or controlled by a third-country person. Since this rule also applies to online platforms, they are effectively prohibited from accepting political advertisements from outside the EU during electoral periods. While this rule does not specifically apply to recommender systems, it is still worth mentioning, as political manipulation through recommender systems has often been attributed to external malicious actors.

130 PAR, recital 6.

131 PAR, recital 6.

132 PAR, art. 3(4). The Regulation explicitly outlines several exclusions from the definition of political advertising. First, political opinion expressed under editorial responsibility, unless they are provided behind remuneration, together with those expressed in an individual capacity, are excluded [PAR, art. 1(2) and 1(3)]. Secondly, messages from official sources of Member States or the EU strictly regarding the organisation and modalities for participating in elections or referendums; public communications intended to provide official information (e.g., press releases); and messages presenting candidates in designated public spaces or in the media provided by law and free of charge, while ensuring the equal treatment of candidates, are also not considered political advertisement [PAR, art. 3(2). See also: recitals 27 and 28]. Moreover, there is a general exclusion for messages of a purely private or purely commercial nature. To assess the nature of the message, all relevant factors must be taken into consideration, including its content, the sponsor, the language used, the context (including the period of dissemination), the objective of the message, the means of transmission, and the targeted audience [PAR, art. 8 and recital 22]. The European Commission may also develop guidelines to ensure the correct interpretation of these criteria. The distinction between private and political opinions is likely to be one of the most contentious issues. See: V. Iaia, *I Complessi Contorni Della Nozione Di Pubblicità Politica Alla Prova Delle Elezioni Europee 2024*, in *MediaLaws*,

message is disseminated in the European Union, independently of the establishment of the provider or sponsor.[133]
Given that this research focuses on recommender systems, restrictions on online targeted political advertising will first be presented, before examining the broader transparency obligations imposed for the various forms of political advertising.

4.1. Lawful Targeted Political Advertisement: Explicit Consent and Restrictions on Profiling

As previously mentioned, the PAR includes specific provisions regulating online targeted political advertising. Targeting is defined as a technique that delivers content selectively, i.e., only to a specific person or group of persons, or through selective exclusions, based on the processing of personal data.[134] The connection between targeting and personal data is made clear from this definition, which is why the main rules of the PAR are built upon the GDPR framework, with their enforcement entrusted to national data protection authorities.
The requirements for the lawful targeting of political advertising online based on the processing of personal data are set out in art. 18 of the PAR, which establishes three key requirements. First, the controller must have collected the personal data directly from the data subject, thereby excluding data obtained from third parties. Second, the data subject must have given "explicit" and "separate" consent to this kind of data processing in accordance with the GDPR. Third, profiling based on the special data listed in art. 9 of the GDPR is strictly prohibited for the purpose of target-

19 June 2024. However, the changes made to the original proposal can provide guidance for interpretation. The preamble of the proposal initially stated that messages on societal or controversial issues which could influence electoral processes should be considered political advertising (Proposal for a Regulation of the European Parliament and of the Council on the transparency and targeting of political advertising, COM/2021/731 final, recital 17), leading to the substantial inclusion of non-remunerated content. See: S. Becker, *Political Negotiations Continue: EU Lawmakers Fail to Agree on Strong Rules for Regulating Political Advertising*, in *European Digital Rights (EDRi)*, 12 October 2023. In contrast, civil society organisations argued that only paid or sponsored political content should be regulated, expressing concerns that including all public interest content, including messages related to abortion, animal protection or human rights, could refrain civil society organisations from generating and disseminating unpaid political messages, ultimately discouraging free speech and activism. Following these debates, lawmakers agreed to keep non-commercial political speech mostly out of scope of the PAR.

[133] PAR, art. 2(1).

[134] PAR, art. 3(11).

ing political advertising.[135] In addition, targeted political advertisement is prohibited when the controller has reasonable certainty that the recipient is at least one year below the voting age.[136] This restriction is justified by the particular vulnerability of younger individuals and the associated risk of influencing them to manipulate public debate.[137]

The consent that online providers must obtain for targeting political advertising must not only meet all the requirements set by GDPR but also be requested separately. The Regulation further specifies that the consent should be required only once, unless there is a substantial change of circumstances, and that revoking consent must not be harder than giving it.[138] Repeatedly prompting users for consent is considered a "dark pattern", as it may nudge them into making a choice they would not have otherwise made.[139] Additionally, the fact that a data subject has voluntarily disclosed their data cannot be considered a sufficient legal ground for political targeting practices.[140] Moreover, to ensure that consent is genuinely freely given, the Regulation reiterates the requirement to provide an "equivalent alternative" to the service offered. Online providers are thus required to allow users to opt out of political advertising while continuing to use their services.[141] In this regard, the preamble explicitly references the *Meta Platforms* case.[142]

Another key rule concerning targeted political advertising is the outright prohibition of profiling based on the "sensitive" data listed in art. 9 of the GDPR.[143] A complete prohibition implies that the exceptions provided by art. 9 GDPR are not applicable in this context and therefore cannot serve as a legitimate basis for data processing.[144] Consequently, providers cannot rely on user consent to target political advertising using sensitive data,[145] aligning this rule with art. 26 of the DSA, which already prohibits

[135] It is explicitly provided that these rules do not apply to non-profit parties and associations for the communication addressed to their members: PAR, art. 18(3).

[136] PAR, art. 18(2).

[137] PAR, recital 82.

[138] PAR, art. 18(4), recital 80.

[139] PAR, recital 75.

[140] PAR, recital 80. Conversely, the GDPR includes voluntary disclosure as legitimate basis for processing special categories of data under art. 9(2), lett. *e)*.

[141] PAR, art. 18(4), recital 81.

[142] See *supra* n 80.

[143] See *supra* n 46.

[144] PAR, recital 77.

[145] S. Becker, *Political Negotiations Continue: EU Lawmakers Fail to Agree on Strong Rules for Regulating Political Advertising,* cit..

profiling on online platforms based on sensitive data for advertising purposes.[146] However, the PAR extends this rule to any online provider of political advertising.
Notably, the PAR explicitly states that the prohibition applies both when special categories of data are collected directly and when they are inferred from the processing of non-special personal data.[147] Furthermore, the prohibition extends to any data revealing such sensitive information, regardless of how they are labelled, and applies independently of the accuracy of the categorisation. However, as mentioned earlier regarding the DSA,[148] distinguishing between different categories of data may not be very effective – a concern shared by certain civil society organisations.[149]

4.2. Transparency Obligations on Political Advertising for Online Platforms

As previously anticipated, the PAR establishes several transparency obligations for political advertising, some of which apply to all providers, while others impose additional requirements on online platforms and for targeted political advertising. This paragraph outlines the main provisions concerning transparency obligations for online platforms in the context of political advertising.
First, all providers of political advertising must require advertisers to declare whether the requested advertising services qualify as "political" under the PAR,[150] and are required to retain records of the information related to the delivery of the requested advertising service for seven years.[151] Publishers of political advertising,[152] a category generally operating at the final stage of the distribution process and including online platforms, must ensure that every political advertisement is accompanied by clear, salient and unambiguous information labelling it as such, and also indi-

[146] See *supra* Section 2.2.

[147] PAR, recital 79.

[148] See *supra* n 64.

[149] A. Allen, *New EU Rules on Political Advertising Set to Have Limited Impact on Advertising Ecosystem*, in *Center for Democracy and Technology*, 20 March 2024.

[150] PAR, art. 8. Any contract subsequently concluded must comply with the rules established by the Regulation and, where an online interface is used, it must be designed in a way that ensures compliance. See: PAR, art. 7(2) and (5).

[151] PAR, art. 9. These records must include the content of the advertisement, the identity of the sponsor, and electoral or political process to which the advertisement relates

[152] PAR, art. 3(13). This category includes services that publish, deliver, or disseminate political advertising through any medium.

cating whether the advertisement is targeted, the identity of the sponsor and, where possible, the entity ultimately controlling the sponsor, as well as the political process to which the advertisement relates.[153] Publishers are responsible for ensuring the completeness of all information and the accuracy of those details under their control,[154] while online providers designated as VLOPs or VLOSEs under the DSA are also required to include such information in the advertising repository mandated by art. 39 of the DSA.[155]

Moreover, publishers must implement mechanisms allowing individuals and organisations to report political advertising that does not comply with the PAR.[156] Publishers qualifying as VLOPs and VLOSEs must additionally handle these notifications diligently, objectively, non-arbitrarily, and without undue delay, informing the notifier of the follow-up. In the month preceding an electoral process, such notifications must be addressed within 48 hours.[157] For data controllers using targeting techniques for online political advertising, art. 19 imposes additional transparency obligations: they must allow individuals to access information about the "logic" and "parameters" of targeting,[158] and are required to conduct an internal risk assessment to evaluate the impact of their targeting mechanism for political advertising on fundamental rights and freedoms.[159]

In addition to these general transparency obligations, researchers, journalists, civil society organizations, electoral observers, and politicians possess

[153] PAR, art. 11. Other information about political advertising must be included in a transparency notice, which must be easily accessible from the sponsored content and including details about the sponsor, the paying entity, the advertising period, the amount of money spent, the origin of the funds, the electoral processes at stake, and information on how to participate to such electoral process. See: PAR, art. 12(1).

[154] If they find any inaccuracies or missing information, they must request corrections from the sponsor. If the sponsor fails to comply, the advertisement must not be published. See: PAR, art. 12(2).

[155] PAR, art. 13(2). A European repository for online political advertisements is also established by the European Commission.

[156] PAR, art. 15.

[157] The short timeframe for content removal during electoral period has been criticised. While intended to prevent the spread of unlawful political advertising, it may create a risk of over-removal of content, which in turn poses an equal threat to the integrity of public debate. See: A. Allen, *New EU Rules on Political Advertising Set to Have Limited Impact on Advertising Ecosystem,* cit.; art. 19, *The Implication of the Proposed EU Political Advertising Regulation for Freedom of Expression*, in *Article 19*, August 2023.

[158] This includes a disclosure on the specifically targeted groups, the categories of personal data used, the targeting mechanism, the reasons for selecting certain parameters, and a link to an internal policy document explaining the targeting techniques.

[159] The European Commission may also, through delegated acts, require the provision of additional information. See: PAR, art. 12(6) and art. 19(5).

the right to request information from publishers, who must provide it free of charge within one month unless providing a reasoned response justifying that they do not possess the requested information or that the request is unclear.[160]

5. Concluding Remarks

Recent regulations on digital platforms, including the DSA, DMA, and the Regulation on Political Advertising, contain several provisions governing recommender systems. Their rules can be generally divided into two categories: those restricting the use and the collection of data, and those enhancing transparency tools.
Regarding the first category, this paper illustrated several restrictions on data processing, resulting in a complex regulatory framework. While most of these rules differ in scope, both in terms of the type of data processing regulated and the entities subject to compliance, overlaps can be observed. The following table (Table 1) summarises the key provisions analysed, aiming to provide a clearer overview of the current regulatory landscape.

Regulation	Type of Data Processing	Compliance Requirements	Subject Entities
GDPR – art. 6	Any data processing	Legitimate basis	All data processors
GDPR – art. 9	Processing special categories of data	Prohibited with exceptions	All data processors
DSA – art. 26	Profiling based on special categories of data for the purpose of ad	PROHIBITED	Online platforms
DSA – art. 28	Profiling minors for the purpose of ad	PROHIBITED	Online platforms

[160] PAR, arts. 17 and 20.

DSA – art. 38	Profiling for recommender systems	Need to provide an alternative	VLOPs and VLOSEs
DMA – art. 5(2)	*Certain data combination practices*	*Need to provide an equivalent alternative*	*Gatekeepers concerning one or more of the core platform services they provide*
PAR – art. 18	*All online targeted political advertising*	*Specific and separate consent + equivalent alternative*	*All data processors*
PAR – art. 18	*Online targeted political ad based on the profiling of special categories of data + on data collected by third parties*	*PROHIBITED*	*All data processors*

Table 1. Restrictions on data processing under different EU regulations affecting digital platforms

This summary highlights how the fundamental principles established by the GDPR in 2016 for personal data processing have evolved along two key directions. First, additional safeguards have been introduced to ensure that user content is genuinely free, thereby reinforcing individual autonomy. In this respect, art. 38 of the DSA,[161] art. 5(2) of the DMA,[162] and art. 18 of the PAR[163] all require digital service providers to offer an "equivalent alternative" that involves less extensive data collection practices. Second, certain types of personal data processing have been outright prohibited, irrespective of user consent. Notably, art. 26 of the DSA and art. 18 of the PAR prohibit profiling for advertising purposes based on the particularly sensitive data identified by the GDPR, while art. 28 prohibits any profiling for advertising purposes when directed at minors.[164] This regulatory shift marks a decisive move away from a purely contractual model based on the formal freedom of the parties, aligning instead with legal frameworks addressing structural contractual asymmetries, such as

[161] See *supra* Section 2.2.

[162] See *supra* Section 3.

[163] See *supra* Section 4.1.

[164] See *supra* Section 2.2.

consumer protection and competition law.

In addition to rules on data processing, a second category of provisions imposes transparency obligations regarding recommender systems, as established in arts. 26 and 27 of the DSA and art. 18 of the PAR.[165] The protection of user privacy is thus complemented with measures aimed at fostering a greater understanding of algorithmic recommendations, thereby enhancing external scrutiny and helping to identify potential bias or manipulation. However, it has been observed that major platforms often fail to provide a meaningful explanation of the reasons underlying the targeting of a specific user.[166] Moreover, the effectiveness of transparency obligations in empowering users has been questioned, as they do not appear to prompt individuals to actively seek information elsewhere,[167] and there is mixed evidence on whether such obligations encourage opting-out behaviours.[168]

Overall, the risk of manipulation is one of the main concerns addressed by these regulations, not only from an individual perspective but also with the broader aim of mitigating societal risks, including threats to the integrity of democratic processes. This explains why individual consent is not considered a sufficient legal basis for certain types of data processing, which are regarded as particularly dangerous, particularly when carried out on a large scale. A major area of concern in this regard is surveillance-based advertising, which relies on extensive data collection, behavioural profiling, predictive analytics, and microtargeting, all with the purpose of influencing user choices, often without their full awareness or meaningful control. While recent regulations have introduced significant limitations to these practices, particularly concerning targeted advertising using sensitive data, some observers argue that they remain insufficiently addressed,[169] since users' vulnerability to microtargeting practices is not only triggered by the special categories of data identified by the GDPR.[170]

Moreover, rules aimed at enhancing users' autonomy by giving them positive control over content recommendations are largely absent. In this con-

---

165 See *supra* respectively: Section 1.1 and Section 3.2.

166 See *supra* Section 2.1.

167 E. Izyumenko et al., *Online Behavioural Advertising, Consumer Empowerment and Fair Competition*, cit., esp. 19.

168 Ibid.; J. Strycharz et al., *Protective Behavior against Personalized Ads: Motivation to Turn Personalization Off*, in *Cyberpsychology: Journal of Psychosocial Research on Cyberspace,* 13(2), 2019.

169 S. Becker - J. Penfrat, *The DSA Fails to Reign in the Most Harmful Digital Platform Businesses – But It Is Still Useful*, cit.; and *How Corporate Lobbying Undermined the EU's Push to Ban Surveillance Ads,* cit.

170 N. Helberger et al., *Choice Architectures in the Digital Economy,* cit.; European Commission, *Commission Staff Working Document | Fitness Check of EU Consumer Law on Digital Fairness,* cit.

text, the DSA has been interpreted as only requiring transparency about existing options to influence recommender parameters, rather than obliging providers to offer such options in the first place.[171] While users can choose to receive less personalised advertising,[172] refuse targeted political advertising,[173] and access an unfiltered version of major platform services,[174] these solutions represent rigid binary choices rather than mechanisms that allow users to actively calibrate recommendation parameters according to their individual preferences.[175] Indeed, a total lack of personalisation could be detrimental to user experience, leading many users to retain the default personalised option.[176] To improve this situation, scholars have proposed allowing users to access a mix of personalised and non-personalised recommendations,[177] or to choose among recommender systems offering different levels of personalisation.[178]

Additional measures to enhance user self-determination in relation to content selection could arguably be required for major platforms (VLOPs and VLOSEs) in the context of systemic risk assessment provisions, which essentially work as "blank rules". Although the European Commission has the power to adopt guidelines in this context,[179] the development of additional measures will mostly but depend on the assessment conducted by the platforms themselves and on the scrutiny exercised by the European Commission. This point reflects a broader consideration: beyond the formal regulatory framework, practical implementation by platforms and enforcement by supervisory authorities will be crucial in determining the actual impact of the examined rules. Indeed, the open-ended nature of risk assessment provisions,[180] the already demonstrated ineffectiveness of

171 See *supra* Section 2.1.

172 DMA, art. 5(1).

173 PAR, art. 18.

174 DSA, art. 38.

175 U. Reviglio - M. Fabbri, *The Regulation of Recommender Systems Under the DSA,* cit.

176 E. Izyumenko et al., *Online Behavioural Advertising, Consumer Empowerment and Fair Competition*, cit., esp. 23.

177 *Ibid.,* esp. 24.

178 J. Harambam – N. Helberger - J. van Hoboken, *Democratizing Algorithmic News Recommenders: How to Materialize Voice in a Technologically Saturated Media Ecosystem*, *Philosophical Transactions of the Royal Society A: Mathematical,* in *Physical and Engineering Sciences,* 376(2133), 2018.

179 DSA, art. 35(3).

180 P. de Hert – P. Hajduk, *EU Cross-Regime Enforcement, Redundancy and Interdependence. Addressing Overlap of Enforcement Structures in the Digital Sphere after Meta.*, in *Technology and Regulation*, 2024, esp. 292.

certain compliance models (such as the *pay-or-consent*),[181] and widespread allegations of non-compliance with the GDPR,[182] all suggest that the paradigm-shifting potential of the examined regulations ultimately depends not only on the substance of the rules, but also on their implementation and the surrounding oversight architecture.[183]

To conclude, the examined rules represent an important step toward strengthening user autonomy in relation to content recommendations, but they require effective implementation and must be complemented by additional measures. Enabling users to partially "personalise the personalisation" of the parameters used by recommender systems appears a particularly promising direction, as it could broaden the information they receive and mitigate bubble effects and wider forms of manipulation. Importantly, this need also arises in relation to other emerging technologies for accessing information, such as generative AI systems.

[181] See *supra* Section 3.

[182] European Center for Digital Rights, *GDPR: A Culture of Non-Compliance?*, in *Noyb*, 2024.

[183] G. De Gregorio – A. Vicinanza, *The Enforcement of European Digital Regulation: Overlaps and Pathways*, in *Yearbook of European Law*, 2026.

Abstract

The paper analyses the advancements and limitations of certain recent EU regulations on digital services in protecting the autonomy of EU citizens online, particularly concerning content transmission and reception. Recommender systems and algorithms play a central role in determining the content users encounter online, including on social media platforms, search engines, and generative AI systems. However, algorithmic content transmission presents significant challenges for EU values, due to its opaque functioning and its reliance on a vast array of personal data, increasing the risk of manipulation. Recent EU regulations, broadly designed to place citizens at the centre of the digital environment, seek to address these concerns through three key mechanisms: (a) specific transparency obligations, (b) reinforced freedom of consent, and (c) prohibition of most high-risk practices. While these new rules represent an important step toward strengthening user autonomy in relation to content recommendations, their effective implementation remains questionable, and they remain limited in providing users with mechanisms to actively shape recommendation parameters.

Keywords

recommender systems – algorithmic systems – digital services – EU digital regulations – algorithmic manipulation