Regulating Political Advertising in the EU

Transparency Without Accountability

Randall Stephenson, Johanna Rinceanu, Marc André Bovermann

eucrim
European Law Forum: Prevention • Investigation • Prosecution

ABSTRACT

In April 2024, the European Union's Regulation on the Transparency and Targeting of Political Advertising (PAR) entered into force. In further efforts to ensure a transparent, safe, predictable and trustworthy online environment within the EU — particularly in the wake of the Cambridge Analytica scandal — the Regulation aims to respond to the dangers and misuse of microtargeting, a sophisticated data-based method of online manipulation. Despite PAR's lofty aspirations, the nature and functions of online manipulation are fraught with more conceptual and regulatory difficulties than it appears to acknowledge or resolve. First, PAR's reliance on outmoded data protection principles and their largely unforeseeable effects on data disposition and aggregation complicate the problem of online user consent. Second, without adopting a broader "supervisory perspective" for identifying harmful microtargeting and interest misalignment, PAR risks endorsing only transparency without accountability. Third, a noticeable regulatory loophole risks prompting a surge in unregulated political advertising through platforms' existing posting functionality. Finally, persistent undertheorising of the underlying nature and effects of microtargeting precludes a comprehensive evaluation of its broader social harms and compatibility with democratic principles. Building on our two previous Digital Iatrogenesis and Differential Diagnosis eucrim publications, this article aims to further highlight and provoke thought and discussion about the more latent and structural challenges of global digital media regulation.

AUTHORS

Randall Stephenson

Senior Researcher; Lecturer (University of Freiburg) / Attorney-at-Law
Max Planck Institute for the Study of Crime, Security and Law, Freiburg i.Br., Germany

Johanna Rinceanu

Senior Researcher; Lecturer (University of Freiburg)
Max Planck Institute for the Study of Crime, Security and Law, Freiburg i.Br., Germany

Marc André Bovermann

Doctoral Researcher
Max Planck Institute for the Study of Crime, Security and Law, Freiburg i.Br., Germany

CITE THIS ARTICLE

Stephenson, R., Rinceanu, J., & Bovermann, M. A. (2025). Regulating political advertising in the EU : Transparency without accountability. Eucrim – European Law Forum: Prevention • Investigation • Prosecution. https://doi.org/10.30709/eucrim-2025-008

Published in eucrim 2025, Vol. 20(1) pp 90 – 97

https://eucrim.eu

ISSN: 1862-6947

I. Introduction

Our contemporary digital media landscape continues to exhibit unforeseen regulatory tensions and harms. Perhaps most revealing is the phenomenon of *microtargeting*,[1] a sophisticated data-based method of online manipulation.[2] Though first arising in commercial settings, the upsurge in such techniques – especially psychographic profiling using machine learning and artificial intelligence (AI)[3] – now encompasses a growing *political* dimension evidenced by the rise of personalised advertising. The threats of this darker side of democracy's "algorithmic turn" are evidenced by the notorious Cambridge Analytica scandal,[4] which exposed the firm's misuse of Facebook data, and its suspected high-jacking of the Brexit referendum and the 2016 US Presidential election.[5] For those initially unpersuaded of microtargeting's dangers and misuse, its reach and powers have only intensified over the years. Besides being an obvious affront to personal autonomy and privacy, its seldom acknowledged aims of extracting hidden data and surprising correlations – and turning such sensitive information into votes – presents unprecedented structural risks to our democracies. Prompting concerns with election insecurity, digital repression, and disinformation,[6] this risky and scarcely understood technology also challenges uncritical use of regulatory approaches based on conventional data protection principles, and continued reliance upon overly-narrow definitions of "data-driven" harms.

The EU has been among the first responders. Its recent Regulation on the Transparency and Targeting of Political Advertising (PAR) entered into force on 9 April 2024.[7] Besides prioritising privacy and personal data protection, PAR's numerous recitals allude to additional objectives of strengthening democracy and safeguarding electoral integrity. Despite Strasburg Court jurisprudence limiting EU regulatory intervention in Member States' approaches to paid political advertising,[8] PAR nonetheless aims to harmonise "transparency" requirements as a central aspect of doing so.[9] This new harmonising measure complements a wide range of existing online regulations, including the Digital Services Act (DSA),[10] the Digital Markets Act (DMA),[11] and the General Data Protection Regulation (GDPR).[12] Overall, as explored in our earlier Digital Iatrogenesis and Differential Diagnosis *eucrim* articles [13]— which aimed to highlight and provoke thought and discussion about the more latent and structural challenges of digital media regulation — PAR purports to add yet another piece to the broader regulatory puzzle of ensuring a safer digital environment in which EU online users' fundamental rights are protected. But does it?

Despite rising awareness of the internet's use as a powerful surveillance, profiling, and advertising tool,[14] scholarship germane to this matter suggests that the nature and functions of online manipulation pose more conceptual and regulatory challenges than PAR acknowledges or resolves. As shown below in Sections II to V, our analysis of this scholarship raises the following four criticisms of PAR's regulatory approach. First, PAR's reliance on outmoded data paradigms and their largely unforeseeable effects on data disposition (and aggregation) complicate the problem of user consent. Second, unless a broader "supervisory perspective" or radical form of third-party-led data oversight is adopted, PAR risks (ironically) endorsing only transparency *without* accountability. Third, a noticeable regulatory loophole risks prompting a surge in unregulated political advertising through platforms' existing posting functionality. Finally, persistent undertheorising of microtargeting's underlying nature and effects precludes a comprehensive evaluation of its broader social harms and compatibility with democratic principles.

II. Nature and Harms of Political Microtargeting

Before assessing PAR's specific regulatory aims and approach, it is important to review the nature of political microtargeting, the vital preconditions for its emergence, and its growing harms to individuals and society.

https://doi.org/10.30709/eucrim-2025-008

1. Nature and emergence of microtargeting

a) Online manipulation

It is essential to first distinguish political microtargeting from other forms of influence. Privacy scholars have coined the term "online manipulation" to highlight the many concealed practices enabled by today's rapidly evolving digital media environment. Whether considering Facebook's microtargeting of vulnerable teenagers, [15] Uber's algorithmic profit nudging of its labour force,[16] or Cambridge Analytica's early use of psychographic profiling to manipulate electoral outcomes,[17] common to each is the exercise of *hidden* influence — the covert subversion of another person's decision-making power. Compared to *persuasion*, which appeals to conscious deliberation, or *coercion*, which materially restricts one's options, *manipulation* exploits another's weaknesses and vulnerabilities to steer their decision-making process towards the manipulator's ends. As a longstanding but underestimated example of online manipulation, microtargeting involves a deliberate *misalignment* of user interests.

b) Informational asymmetries and *laissez-faire* data disposition

While almost anyone can deceive (e.g. commit fraud), online manipulation requires a large power or knowledge imbalance rendering individuals susceptible to exploitation. It is therefore not surprising that microtargeting flourishes in today's digital media ecology, which is typified by acute *informational asymmetries* and a particularly *laissez-faire* regulatory approach to the flow and protection of disclosed information. Besides the data we shed "voluntarily" on social media, digital platforms' dynamic, interactive, intrusive, and highly-personalisable choice architecture makes them an unprecedentedly powerful tool for hyper-targeted manipulation.

c) Outmoded data paradigms

This informational imbalance gives rise to a distinct regulatory anomaly, where data traffickers and digital platforms, whose interests may not align with those of their users, have both the intimate knowledge and relational proximity necessary to *manipulate* them commercially and politically. This anomaly is effectively explained by the principle of "privacy-as-concealment".[18] Described as the "original sin" of the digital market, [19] this equates privacy with consumers' ability to conceal information. Once information is "disclosed" online, users are treated as having *relinquished* their privacy and any reasonable expectation of data control. Except for persons having directly contracted with consumer-facing firms, disclosed information is generally *not* regulated and may be aggregated and sold freely.[20] This has become problematic as data traffickers' secondary use of information lacks transparency, and thereby harms users in potentially uncontrollable ways. These data traffickers (or aggregators) have no interaction or privity of contract with persons they target, and arguably represent the "real engine" of online manipulation. Scholars caution that focussing regulatory efforts only on platforms' Terms of Use merely facilitates outsourcing poor data practices to ungoverned third parties.[21]

2. From explicit to informed consent

Making matters worse, the largely unforeseeable effects of informational asymmetries and data disposition also complicate issues of consent, provoking calls for more stringent requirements analogous to the medical doctrine of *informed consent*.[22] According to this doctrine, consent must be "knowledgeable" in some meaningful sense in order to ensure awareness and to protect an individual's ability to make autonomous decisions. Much like physicians disclosing detailed information vital to a patient's decision about proposed treatment and interventions, digital platforms should provide online users with a summary in plain language

of potential risks and benefits associated with data disposition (including political microtargeting).[23] This would enable users to give meaningful consent to any data disclosure. "Explicit consent", hence, is not sufficient, particularly if users are unaware of a potentially harmful secondary (or even tertiary) use of their data. Arguably only informed consent is capable of mitigating such informational imbalances (which enable digital platforms to *exploit* their data subjects), and protecting the self-determination of online users.

3. Microtargeting as a data-driven harm

Lastly, reflexively framing data misuse within individual privacy norms is increasingly seen as an "outdated paradigm" that overlooks rising structural threats to democracy. Since election interference and voter manipulation are harms affecting public interests, privacy is no longer just an individual issue, but a *networked* phenomenon requiring networked solutions.[24] Alongside calls to reconceptualise cybersecurity law and the "strict tangibility approach" to data-breach jurisprudence,[25] scholars have endorsed a *collective perspective* for regulating data-driven harms.[26] Aiming at "meaningful transparency",[27] this requires far more than just disclosing ad-targeting criteria or funding details, or creating public ad-databases divorced from the harmful effects of data loops. Rather, a broader "supervisory perspective" is needed to *correlate* outgoing user information with incoming personalised content in order to identify harmful commercial and political microtargeting and interest misalignment.[28] This heightened informational scrutiny, however, leads to a larger regulatory dilemma. As a prominent free speech scholar observed already in 2016, "the more speech-protective the government's policy, the more hands-on the government's approach will need to be".[29] That is to say, a regulatory dilemma arises owing to such extreme forms of informational transparency. The very "supervisory perspective" needed for identifying and exposing microtargeting and interest misalignment unfortunately also confers unprecedented possibilities for privatised governmental censorship and regulatory capture. As opposed to earlier predigital eras, regulating online speech invariably places the government in our proverbial editorial office. Ironically, without this extreme level of informational surveillance, regulatory proposals such as PAR risk only endorsing transparency *without* accountability.

III. PAR's Essential Aims and Features

1. Regulatory aims

PAR aims to contribute to the proper functioning of the EU's internal market for political advertising, and to protect fundamental rights and freedoms – particularly the right to privacy and the protection of personal data (Art. 1(4) PAR). Responding to digital technologies and the use of social media in electoral campaigning that offer political actors massive reach at low cost,[30] PAR introduces harmonised transparency rules regarding online political campaigning for each of the EU's 27 Member States.

2. Regulatory features

Despite its apparent complexity, PAR comprises four main regulatory features: (1) labelling and transparency requirements; (2) establishing a public database for political ads; (3) restricting political microtargeting and foreign electoral interference; and (4) sanctioning non-compliance.

First, political ads must be clearly labelled and include an easily retrievable notice disclosing details such as its sponsor, any controlling entity, the electoral process to which the ad refers, the amounts paid, and any microtargeting or ad-delivery methods used (Arts. 11, 12 PAR). Notices must be accessible contemporaneously with the original ad (e.g. via QR-Code) and (like DSA) provide a "notice-and-action" mechanism for reporting non-compliant ads (Art. 15 PAR).

Second, both the ad and notice must be submitted to a European repository established by the Commission (Art. 13 PAR) – a public database available in machine-readable format. If the publisher is a very large online platform (VLOP) within the meaning of Art. 33 DSA, it can use its general ad repository. However, as with all PAR record-keeping, VLOPs must facilitate access for seven years after the ad was last posted (Arts. 12(4), 13 PAR).

Third, PAR permits targeted online political advertising, subject to three conditions (Art. 18 PAR): (1) the controller (i.e. data processing entity) must collect the personal data *directly* from the subject; (2) the latter must *explicitly consent* to the processing of their personal data for political advertising; and (3) the processing cannot involve "profiling" (i.e. "any form of automated processing of personal data") using special data categories (e.g. race or ethnicity, political opinions, etc.) as referred to in Art. 9(1) GDPR. Importantly, PAR prohibits political microtargeting to minors (Art. 18(2) PAR). Foreign electoral interference is restricted by a so-called "silence period", which prohibits provision of political advertising services to non-EU or otherwise unqualified foreign sponsors (or service providers) within three months of an election or referendum organised at EU, national, or regional levels (Art. 5(2) PAR).

Fourth, like the DSA, PAR imposes indexed financial penalties for non-compliance. Fines must not exceed 6% of the annual income or budget of the sponsor or the provider of political advertising services (as applicable), or 6% of the sponsor's or provider's annual worldwide turnover in the preceding financial year (Art. 25 PAR).

IV. Political Advertising's "Regulatory Loophole"

This is about where regulatory certainties end as PAR's scope of application seems unclear in one important respect. A close look at the definition of "political advertising service" in Art. 3(5) PAR reveals a drafting irregularity that appears to obscure PAR's regulatory reach. It reads:

> 'political advertising service' means a service consisting of political advertising with the exception of an online 'intermediary service', as defined in Article 3, point (g), of Regulation (EU) 2022/2065, that is provided without consideration, for the preparation, placement, promotion, publication, delivery or dissemination for the specific message.

The source of ambiguity originates from the attempt to exempt "intermediary services" from the definition of "political advertising service". Notably, Art. 3(g) DSA divides "intermediary services" into three distinct categories: (1) "mere conduit" service; (2) "caching" service; and (3) "hosting" service (e.g. social media platforms).

Difficulty arises when attempting to discern what the words "provided without consideration" modify. If interpreted to restrict the definition of "political advertising service", a tension arises between the categorical exclusion of conduit, caching, and hosting intermediaries, and the further obligation to saddle "political advertising *publishers*" (defined in (Art. 3(13)) with the full suite of transparency obligations under PAR. While mere conduit and caching services (i.e. non-curatorial) – along with purely private and purely commercial messages – are clearly and understandably exempt from PAR's application, exempting "hosting services" captured by the definition of "political advertising publisher" makes considerably less sense.

By contrast, if "provided without consideration" modifies the exempted online "intermediary services" (under DSA), a crucial policy factor comes back into focus. Specifically, this interpretation is consistent with the reassurance in Recital 47 that PAR should *not* apply to *unpaid* content uploaded by users of an online intermediary (e.g. hosting) service, such as a social media platform. In short: no paid "political advertising service", no transparency obligations. So, why rely on political advertising services when one could simply

https://doi.org/10.30709/eucrim-2025-008

use a platform's basic posting functionality? As the following two examples show, this regulatory loophole has already generated serious socio-political consequences.

First, as political campaigns increasingly take place in the digital sphere, modern electioneering is not merely conducted through ad-distribution services, but involves direct engagement with potential voters on politicians' home turf – namely, on their own private social media feeds. The political right has mastered this type of voter engagement.[31] In Germany, a good example is *Maximilian Krah* of the Alternative für Deutschland (AfD) party, who has gathered a huge audience on TikTok. As Krah's growing popularity and the last German federal election have shown,[32] PAR risks inadvertently prompting a surge in unregulated political advertising through the existing posting function on platforms.

Second, the use of TikTok by Romanian presidential candidate *Călin Georgescu* has sparked a debate about digital campaigning in the context of the last Romanian presidential election. The election was annulled by the Romanian Constitutional Court.[33] It commented on Georgescu's use of his personal TikTok account to influence voters and held that the presidential electoral process had been subverted. The Court emphasised that Georgescu had unfairly benefitted from aggressively promoting his political messages through digital platforms' algorithms, which had effectively circumvented the electoral legislation and led to misinformation and voter manipulation.[34]

In the end, despite PAR's explicit commitment to "fully respect fundamental rights" in its objectives and application, this regulatory loophole not only inadvertently emboldens right-wing populist parties and candidates, but also appears to pose a considerable threat to the openness and accountability of EU electoral mechanisms.

V. Undertheorising Democratic Free Speech Rationales

Besides uncertainties about its application, PAR also raises vital fundamental rights concerns. As commentators acknowledged early on in the regulatory debate about online manipulation, "[b]ecause of free speech norms, policymakers must tread carefully when regulating political speech, and when regulating political advertising".[35] While the scholarly literature on the nature and suitability of political microtargeting — and "online manipulation" more generally — invokes conventional free speech conceptions of autonomy, chilling effects,[36] and participatory and deliberative democracy, this scholarly discussion remains undertheorised and therefore regulatorily deficient in one key respect. Specifically, as with other areas of freedom of expression regulation — public libel law[37] being especially illustrative — existing scholarship consistently overlooks perhaps the most relevant free expression justification for regulating the threats of political microtargeting: the "checking function" rationale and its link to democratic accountability.[38] This undertheorising manifests in two distinct but related ways pertinent to regulators on both sides of the Atlantic.

1. Conflating democratic free-speech values

The first form of undertheorising involves scholarly attempts to expand "data-driven" harms to include those affecting democracy more broadly, where the scalable effects of online manipulation are routinely (and imprudently) masked by subsuming the checking function within classic *Meiklejohnian* notions of deliberative democracy.[39] The upshot is a disproportionate focus on free speech's "information conduit" role in *imparting* and *receiving* information — as guaranteed under Art. 10 of the European Convention on Human Rights (ECHR) and Art. 11 of the Charter of Fundamental Rights of the European Union (Charter) — rather than minding the impact of PAR's "harmonising" strategy on the institutional press' vital *watchdog* role of

holding power to account. Whether purporting to assess political microtargeting's advantages and disadvantages,[40] or the inevitable "trade-offs" between different and often conflicting democratic values and ideas,[41] a vital shortcoming of regulatory analyses is the systematic disregard of the checking function rationale — a crucial component in achieving a precise regulatory balance between competing rights, interests, and values. In effect, by overlooking the checking function and its connection to the press' vital but waning "fourth estate" role,[42] when one explicitly acknowledges political microtargeting's hidden and manipulative nature, regulatory evaluations necessarily understate its harmful socio-political effects on democracy.

This undertheorising can have serious and disruptive regulatory and doctrinal outcomes. As recent comparative law scholarship has revealed, "our ability to diagnose and understand contemporary problems falters when we encounter breakdowns in the theory-doctrine interface".[43] As reported in the comparable context of online defamation, our strongest guarantee of sound regulation and doctrine "depends on ensuring a complete inventory of fully articulated free expression justifications carefully applied to relevant issues and disputes. The effects of the Internet, however measured, cannot sidestep this basic requirement".[44] As threatened in the context of PAR's regulatory approach to political microtargeting, at stake is no less than the likelihood of inadvertently promoting arbitrary regulatory measures at odds with our most fundamental political values.

2. Political microtargeting as "speech"

A further form of undertheorising is raised by reflexively interpreting political microtargeting as a protected form of political communication or "speech", a disquieting scholarly approach seen both in Europe and North America.[45] Importantly, whether in either context, if microtargeting is uncritically presumed to be political "speech", our regulatory focus will remain elsewhere than on tracking its fundamental inconsistency with underlying freedom of expression justifications, particularly the checking function rationale.

As a recent commentary on the nature and threats of political microtargeting has shown,[46] a key component of its proper regulation will be engaging in a careful assessment of its doctrinal and theoretical status as a form of protected speech. Despite temptations to *equate* political microtargeting with political communication, or to interpret it in a *Meiklejohnian* manner consistent with notions of deliberative democracy and the basic structure of Art. 10 ECHR and Art. 11 of the Charter (i.e. as the dyadic *imparting* and *receiving* of information),[47] a recent vein of scholarship on algorithms' status as "protected speech" has sensibly advised *against* such presumptive views.

In the context of US First Amendment doctrine, Columbia Law Professor *Tim Wu* has convincingly argued that the law contains a "de facto *functionality* doctrine" that "must be central to any consideration of [regulating] machine speech".[48] In other words, in the absence of any suspicious governmental censorship motives, this "functionality doctrine" will be the main dividing line between constitutionally protected "speech" and other forms of communication. This doctrine, according to *Wu*, operates in two distinct ways.

The first category of information excluded from First Amendment protection is where it is simply "too distant or mechanical to be speech".[49] *Wu* explains that this covers those who handle or transform information in a *non-curatorial* manner "usually lacking specific choices as to content, [who] lack specific knowledge as to what they are handling, or do not identify as the publisher of the information".[50] Telephone services, for example, have historically fallen outside the ambit of free speech rights as they were treated as essential utilities, not as "speakers". The second category of excluded speech are "communicative tools", where the information conveyed is *functional*—viz., it performs some task *other than* the communication of ideas. *Wu* references both ordinary maps and navigational charts as paradigmatic examples of such "communicative tools". In the end, the largely unstated reasons courts give for denying constitutional protection to non-curatorial carriers or communicative tools, is their reluctance to extend free speech regulation into areas

where other motivations are paramount and/or to quell the opportunism of lawyers trying to use the Constitution to achieve goals unrelated to speech.[51]

Furthermore, without incorporating this functionality doctrine as a missing regulatory piece of the puzzle, uncritical and reflexive application of the now decades-old "code is speech"- model will continue to yield results both absurd and disruptive that cannot be taken seriously. Interestingly, in a bid to "roll back" the regulatory overestimation of "[…] the significance of computer code's superficial resemblance to words on a page",[52] and to prevent further overprotection of computer code secured during the first wave of internet cases, free speech scholar *Kyle Langvardt* has recommended adopting a "threshold test" patterned on Wu's "functionality doctrine". This would work by "quarantining" new code cases (e.g. those involving algorithms and machine learning) from "mainline First Amendment doctrine so that they are not decided under the same set of [overbroad] tests".[53] As this discussion shows, deciding that political microtargeting constitutes "political speech" involves a considerably more complex and careful analysis, whether in European or American jurisdictions.

At last, just as framing data misuse within conventional privacy norms has been criticised as an "outmoded paradigm" that neglects growing harms to democracies, this narrowing of democratic free speech rationales (and over-constitutionalising of computer code) risks greatly limiting our understanding of the full extent and severity of political microtargeting. This theoretical oversight obscures the reasons *why* we should be concerned with its regulation and/or outright prohibition in the first place.

VI. Conclusion

Which brings us full circle. Viewed in light of the scholarly foundations of microtargeting, PAR's regulatory approach (and even mere existence) raises many questions, in the end overpromising and underdelivering on its avowed policy aims. First, despite the apparent lack of regulatory fragmentation that would justify the EU's push to "harmonise" transparency obligations,[54] PAR's reliance on conventional data protection paradigms and limited regulatory reach effectively endorses only transparency without accountability. With the exception of bald compliance (re)assurances in regulated entities' annual reports, harmful political microtargeting and interest misalignment will in all likelihood remain undetected unless a collective perspective that correlates outgoing user data with incoming personalised content is adopted. Second, PAR continues to overlook the insufficiency of existing user "consent" requirements. Whether confronted with personalised content or not, it remains unclear how users can meaningfully (let alone "explicitly") consent to unforeseeable secondary (and even tertiary) data aggregation, disposition, and manipulation. Third, as evidenced by Maximilian Krah and Călin Georgescu's use of their private social media feeds, a noticeable regulatory loophole risks prompting a surge in unregulated political advertising through platforms' existing posting functionality. Finally, this article has explained that persistent undertheorising of microtargeting's harmful effects precludes a full evaluation of its compatibility with democratic principles. While digital media regulation inevitably involves trade-offs between different and often competing democratic values, it is difficult to determine which regulatory approach best serves democracy, or even which understanding of democracy should prevail, without fully canvassing the nature and implications of *each* rationale. Under such circumstances, PAR's overall approach, expected benefits, and effects are in the end far from clear.

---

1. See generally N. Witzleb, M. Paterson and J. Richardson, *Big Data, Political Campaigning and the Law: Democracy and Privacy in the Age of Micro-Targeting*, 2021.↩
2. See D. Susser, B. Roessler and H. Nissenbaum, "Online Manipulation: Hidden Influences in a Digital World", (2019) 4 *Georgetown Law Technology Review*, 1.↩
3. D. Susser and others, *op. cit.* (n. 2), 9–12. See also "Psychographic Profiling: The Secret to Enhanced Marketing", *Sagacity*, <https://www.saga-citysolutions.co.uk/about/news-and-blog/psychographic-profiling-the-secret-to-enhanced-marketing/>. All hyperlinks in this article were last accessed on 4 July 2025.↩

4. See e.g., A. Gurumurthy and D. Bharthur, "Democracy and the Algorithmic Turn", (2018) 27 *SUR – International Journal on Human Rights*, 39.↩
5. See e.g., A. Chan, "Cambridge Analytica and our Lives Inside the Surveillance Machine", *The New Yorker*, 21 March 2018, <https://www.newyorker.com/tech/annals-of-technology/cambridge-analytica-and-our-lives-inside-the-surveillance-machine>.↩
6. See generally S. Shackelford, A. Raymond, A. Stemler and C. Loyle, "Defending Democracy: Taking Stock of the Global Fight Against Digital Repression, Disinformation, and Election Insecurity", (2020) 77 *Washington & Lee Law Review*, 1747.↩
7. Regulation (EU) 2024/900 of the European Parliament and of the Council of 13 March 2024 on the transparency of political advertising, *OJ* L, 2024/900, 20.3.2024.↩
8. M. Zeno van Drunen, N. Helberger and R. Ó Fathaigh, "The beginning of EU political advertising law: unifying democratic visions through the internal market", (2022) *30 International Journal of Law and Information Technology*, 181, 182, citing *Animal Defenders International v United Kingdom* [2013] ECtHR 48876/08 [123]; *VgT Verein gegen Tierfabriken v Switzerland* [2001] ECtHR 24699/94 [70]; *TV Vest* [2008] ECtHR 21132/05 [67].↩
9. M. Zeno van Drunen and others, *op. cit.* (n. 8), 195–96. The authors rightly noted that there appears to be insufficient regulatory fragmentation to justify the EU's push to "harmonise" transparency obligations. Hypothesising that "transparency [is] an area Member States were most likely to accept European Commission intervention," they emphasised that "[t]his still leaves the question, unaddressed by the impact statement, why the regulation of transparency is available for harmonization but other areas not […]" (p. 196). Given the large scope of discretion granted to Member States, PAR would appear to be regulating their domestic political affairs under the mere guise of transparency.↩
10. 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) [2022] OJ LI277/1.↩
11. 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).↩
12. 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).↩
13. R. Stephenson and J. Rinceanu, "Digital Iatrogenesis: Towards an Integrative Model of Internet Regulation", (2023) 1 *eucrim*, 73; R. Stephenson and J. Rinceanu, "Differential Diagnosis in Online Regulation: Reframing Canada's 'Systems-Based' Approach", (2024) 3 *eucrim*, 245.↩
14. See S. Zuboff, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*, 2019.↩
15. S. Levin, "Facebook told advertisers it can identify teens feeling 'insecure' and 'worthless'", *The Guardian*, 1 May 2017, <https://www.theguardian.com/technology/2017/may/01/facebook-advertising-data-insecure-teens>.↩
16. Z. Muller, "Algorithmic Harms to Workers in the Platform Economy: The Case of Uber", (2020) 53 *Columbia Journal of Law and Social Problems*, 167.↩
17. S. Halpern, "Cambridge Analytica and the Perils of Psychographics", *The New Yorker*, 30 March 2018, <https://www.newyorker.com/news/news-desk/cambridge-analytica-and-the-perils-of-psychographics>.↩
18. K. Martin, "Manipulation, Privacy, and Choice", (2022) 23 *North Carolina Journal of Law & Technology*, 452, 493.↩
19. K. Martin, *op. cit.* (n. 18), 494.↩
20. Emanuela Podda, "Shedding Light on the Legal Approach to Aggregate Data Under the GDPR & the FFDR" (Conference of European Statisticians – Expert Meeting on Statistical Data Confidentiality, Poland, December 2021). Citing Recital 162 of the GDPR, Podda states that "aggregate data is the result of personal data processing for statistical purpose (output data) and it is considered non-personal data". Interestingly, this position appears to be in tension with the principle of "integrity and confidentiality" under Art. 5(1)(f) GDPR.↩
21. K. Martin, *op. cit.* (n. 17), 520.↩
22. K. Rhum, "Information Fiduciaries and Political Microtargeting: A Legal Framework for Regulating Political Advertising on Digital Platforms", (2021) 115 *Northwestern University Law Review*, 1829, 1868.↩
23. K. Rhum, *op. cit.* (n. 22), 1868.↩
24. See J. Dawson, "Microtargeting as Information Warfare", (2021) 6 *Cyber Defense Review*, 63, 72.↩
25. See I. Kilovaty, "Legally Cognizable Manipulation", (2019) 34 *Berkeley Technology Law Journal*, 449, 459–60.↩
26. See A. Gordon-Tapeiro, A. Wood and K. Ligett, "The Case for Establishing a Collective Perspective to Address the Harms of Platform Personalization", (2023) 25 *Vanderbilt Journal of Entertainment and Technology Law*, 635.↩
27. A. Gordon-Tapeiro and others, *op. cit.* (n. 26), 679.↩
28. A. Gordon-Tapeiro and others, *op. cit.* (n. 26), 682.↩
29. See K. Langvardt, "Regulating Online Content Moderation", (2018) 106 *Georgetown Law Journal*, 1353, 1363.↩
30. K. Wirthwein, M. Cabañas, F. Di Nunno and L. Rea, "EU Regulation on Transparency and Targeting of Political Advertising – Could the New Legislation be Effective at Stopping Populism?", (FEPS Policy Study, April 2024), <https://feps-europe.eu/wp-content/uploads/2024/05/PS-EU-regulation-on-transparency-DIGITAL.pdf>.↩
31. See "So ungleich war der Bundestagswahlkampf im Netz", *Tagesschau*, 6 March 2025, <https://www.tagesschau.de/investigativ/bundestagswahl-wahlwerbung-instagram-facebook-parteien-budget-100.html>.↩
32. See e.g., Hans Pfeifer, "AfD: How Germany's far right won over young voters", *Deutsche Welle*, 10 June 2024, <https://www.dw.com/en/afd-how-germanys-far-right-won-over-young-voters/a-69324954>.↩
33. See Constitutional Court of Romania, decision no. 32/2024, published in M. Of. no. 1231 from 6 December 2024; ECtHR, 6 March 2025, *Georgescu v Romania*, Appl. no. 37327/24.↩
34. See Constitutional Court of Romania, *op. cit.* (n. 33), para. 14.↩
35. See generally F.J. Zuiderveen Borgesius, J. Möller, S. Kruikemeier, R. Ó Fathaigh, K. Irion, T. Dobber, B. Bodo and C. de Vreese, "Online Political Microtargeting: Promises and Threats for Democracy", (2018) 14 *Utrecht Law Review*, 82, where the authors' early attempt to assess the impact of political microtargeting is fundamentally led astray by overlooking the independent checking function rationale.↩
36. See e.g., *Baggett v Bullitt*, 377 US 360 (1964), where the US Supreme Court struck down a Washington state law mandating loyalty oaths for state employees, asserting that the "the threat of sanctions may deter […] almost as potently as the actual application of sanctions".↩

37. See e.g., R. Stephenson, *A Crisis of Democratic Accountability: Public Libel Law and the Checking Function of the Press*, 2018.↩
38. See V. Blasi, "The Checking Value in First Amendment Theory", (1977) 2 *American Bar Foundation Research Journal*, 521.↩
39. See A. Meiklejohn, "Free Speech and its Relation to Self-Government", in A. Meiklejohn, *Political Freedom: The Constitutional Powers of the People*, p. 1948.↩
40. F.J. Zuiderveen and others, *op. cit.* (n. 35).↩
41. D. Kreiss and B. Barrett, "Democratic Tradeoffs: Platforms and Political Advertising", (2020) 16 *Ohio State Technology Law Journal*, 495.↩
42. For well-documented accounts of the recent crisis of journalism, see e.g., A.S. Jones, *Losing the News: The Future of the News that Feeds Democracy*, 2009; R.W. McChesney and J. Nichols, *The Death and Life of American Journalism: The Media Revolution That Will Begin the World Again*, 2010; David AL Levy and Rasmus Kleis Nielsen (eds.), *The Changing Business of Journalism and Its Implications for Democracy*, 2010; L.C. Bollinger, *Uninhibited, Robust, and Wide-Open: A Free Press for a New Century*, 2010, ch 3; R.W. McChesney and V. Pickard (eds.), *Will the Last Reporter Please Turn out the Lights: The Collapse of Journalism and What can be Done to Fix It*, 2011.↩
43. See R. Stephenson, "Restoring Accountability in Freedom of Expression Theory: Public Libel Law and Radical Whig Ideology", (2018) 56 *Osgoode Hall Law Journal*, 17, 57.↩
44. Stephenson, *op. cit.* (n. 43), 58.↩
45. T. Dobber, R. Ó Fathaigh and F.J. Zuiderveen Borgesius, "The Regulation of Online Political Micro-Targeting in Europe", (2019) 8(4) *Internet Policy Review*, 1, 7.↩
46. Dobber and others, *op. cit.* (n. 45).↩
47. Dobber and others, *op. cit.* (n. 45), 7.↩
48. T. Wu, "Machine Speech", (2013) 161 *University of Pennsylvania Law Review*, 1495, 1497. For an opposing view, see S.M. Benjamin, "Algorithms and Speech", (2013) 161 *University of Pennsylvania Law Review*, 1445, where the author maintains that algorithmic-based outputs that entail substantive editorial decisions are "speech" for First Amendment purposes.↩
49. Wu, *op. cit.* (n. 48), 1521.↩
50. Wu, *op. cit.* (n. 48), 1521.↩
51. Wu, *op. cit.* (n. 48), 1524.↩
52. K. Langvardt, "Four Modes of Speech Protection for Algorithms", in W. Barfield (ed.), *Cambridge Handbook of the Law of Algorithms*, 2020, 543, 557.↩
53. Langvardt, *op. cit.* (n. 52), 552.↩
54. M. Zeno van Drunen and others, *op. cit.* (n. 8), 195–96.↩

ABOUT EUCRIM
eucrim is the leading journal serving as a European forum for insight and debate on criminal and "criministrative" law. For over 20 years, it has brought together practitioners, academics, and policymakers to exchange ideas and shape the future of European justice. From its inception, eucrim has placed focus on the protection of the EU's financial interests – a key driver of European integration in "criministrative" justice policy.
Editorially reviewed articles published in English, French, or German, are complemented by timely news and analysis of legal and policy developments across Europe.
All content is freely accessible at https://eucrim.eu, with four online and print issues published annually.

Stay informed by emailing to eucrim-subscribe@csl.mpg.de to receive alerts for new releases.
The project is co-financed by the Union Anti-Fraud Programme (UAFP), managed by the European Anti-Fraud Office (OLAF).

Co-funded by the European Union