

The Great Data Standoff: Researchers vs. Platforms Under the Digital Services Act

Catalina Goanta¹, Savvas Zannettou², Rishabh Kaushal³, Jacob van de Kerkhof^{4*}, Thales Bertaglia¹, Taylor Annabell⁵, Haoyang Gui¹, Gerasimos Spanakis⁶, Adriana Iamnitchi⁶

¹Utrecht University

²TU Delft

³Indira Gandhi Delhi Technical University for Women

⁴De Brauw Blackstone Westbroek

⁵Cardiff University

⁶Maastricht University

e.c.goanta@uu.nl, s.zannettou@tudelft.nl, rishabhkaushal@igdtuw.ac.in, j.j.w.vandekerkhof@uu.nl, t.f.costabertaglia@uu.nl, annabellt@cardiff.ac.uk, h.gui@uu.nl, jerry.spanakis@maastrichtuniversity.nl, a.iamnitchi@maastrichtuniversity.nl

Abstract

To facilitate accountability and transparency, the Digital Services Act (DSA) sets up a process through which Very Large Online Platforms (VLOPs) need to grant vetted researchers access to their internal data (Article 40(4)). Although expectations are high for this mechanism to provide unprecedented data access as part of the DSA compliance obligations, operationalising it is challenging for two reasons. First, data access is only available for research on systemic risks affecting European citizens, a concept that still raises high levels of legal uncertainty. Second, data access suffers from an inherent standoff problem. Researchers need to request specific data but are not in a position to know all internal data collected, processed and stored by VLOPs, who, in turn, expect and demand data specificity for potential access. To contribute to the discussion of how Article 40 can be interpreted and applied, we provide a concrete illustration of what data access can look like in a real-world systemic risk case study. Our goal is not only to share with the research community at large a scenario for reflection, but also to provide hands-on insights into what type of data platforms may be required to share through the DSA. To this end, we focus on the 2024 Romanian presidential election interference incident, as this event is the first of its kind to trigger systemic risk investigations by the European Commission. In the context of these elections, one candidate is said to have benefited from TikTok algorithmic amplification through a complex and multilayered dis- and misinformation campaign. By analysing this incident, we can concretely comprehend election-related systemic risk in order to explore practical research tasks and compare necessary data with available TikTok data. In particular, our study makes two contributions: (i) we combine insights from law, computer science and platform governance to shed light on the complexities of studying systemic risks in the context of election interference, focusing on two relevant factors: platform manipulation and hidden advertising; and (ii) we provide practical insights into various categories of available data for the study of TikTok, based on platform documentation,

data donations and TikTok's Research API.

Introduction

The Digital Services Act (DSA) has introduced new transparency obligations for Very Large Online Platforms (VLOPs) offering their services to European Union (EU) users. One of these obligations is to grant access to their internal data to researchers through a procedure established by the DSA (Article 40) and further detailed in the accompanying Delegated Act (DA). While Article 40 promises to provide unprecedented data access, two main obstacles hinder operationalisation. First, data access is only granted for the study of systemic risks (Article 40(4) DSA). Systemic risks are a new concept in European platform regulation, and although they are somewhat defined in the DSA (Article 34), a lot of uncertainty remains regarding their practical interpretation. Second, VLOPs are opaque organisations, so there is no way of knowing what data they actually gather, infer, process, and use. However, researchers will be expected to specify the data they require. Not having a full picture of the data VLOPs have can render data access less effective than intended. In light of these major interpretational and operational limitations, data access under Article 40 DSA remains, for the time being and most part, shrouded in mystery.

To contribute to the discussion of how Article 40 can be interpreted and applied, we provide a concrete illustration of what data access can look like in a real-world systemic risk case study. Our goal is not only to share with the research community at large a scenario for reflection, but also to provide hands-on insights into what type of data platforms may be required to share through the DSA. To this end, we focus on the 2024 Romanian presidential election interference incident (Ross and Popoviciu 2024) as this event is the first of its kind to trigger systemic risk investigations by the European Commission (Commission 2024). In the context of these elections, one candidate is said to have benefited from TikTok algorithmic amplification through a complex

*Work completed while employed by Utrecht University
Copyright © 2026, Association for the Advancement of Artificial Intelligence (www.aaai.org). All rights reserved.

and multilayered coordinated dis- and misinformation campaign. By analysing this incident, we explore practical research tasks and compare necessary data with available TikTok data. In particular, our study makes two contributions: (i) we combine insights from law, computer science, and platform governance to highlight the complexities of studying systemic risks in the context of election interference, focusing on two relevant factors: platform manipulation and hidden advertising; and (ii) we provide comprehensive and practical insights into various categories of available data for the study of TikTok, based on platform documentation, data donations, and TikTok's Research API.

Data Access and Systemic Risks Under the Digital Services Act

Article 40 DSA is a novel transparency instrument, seeking to build on existing measures such as transparency reporting (Urman and Makhortykh 2023; Kosta and Brewczyńska 2019), statements of reasons (Leerssen 2023) and the DSA transparency database (Kaushal et al. 2024). It gives Digital Services Coordinators (DSCs, Article 40(1) DSA) and 'vetted researchers' (Article 40(8) DSA) unprecedented data access to online platforms to unpack opaque algorithmic systems (Leerssen 2024; Pasquale 2016). Particularly in a landscape where platforms (including social media platforms) are tightening their control over data and deprecating APIs,¹ Article 40 DSA makes a lofty promise. However, two main considerations severely restrict what may otherwise be seen as a new tool for wide platform transparency.

First, the procedure to acquire data access through Article 40 is complex. It is outlined in the DA, an instrument adopted by the European Commission to further clarify who can apply for data access, and under which circumstances. Interested researchers must submit an application that contains, amongst others, a description of the research project, the research question, the systemic risks or mitigation measures studied, and the planned research activities (Article 8 DA) with the DSC of their Member State, or with the DSC of the Member State of establishment of the platform. Requests may be submitted both at the Member State of establishment of the researcher and that of the platform, but the former has to forward the request to the latter: the DSC of the Member State of establishment of the platform is the only authority with jurisdiction in these cases. After submission of the data access application, the DSC of the Member State of establishment of the platform formulates a reasoned request, in which it determines the access modalities – the avenue through which the data provider grants data – and forwards the application to the online platform (Article 9 and 10 DA). The platform then decides whether it grants the request or submits amendments to the DSC (Article 40(5) DSA). After an optional mediation period (Article 13 DA), the data access request is completed and access should be granted. The role of the DSC in this process is crucial, as it defines the final request submitted to the platform. As such,

¹For example, in 2024 Meta discontinued CrowdTangle: <https://transparency.meta.com/en-gb/researchtools/other-datasets/crowdtangle/>.

the likelihood of a successful data application can be contingent on aligning that application with the DSC's interests, and whether the DSC has the operational capacity to address the application. It is likely that the DSCs of establishment of most VLOPs (Ireland and the Netherlands) will be subject to most applications, which could lead to a case overload paralysing public authorities.

Second, data access is conditional on making a contribution to the detection, identification, and understanding of systemic risks in the EU or assessing whether those risks are sufficiently mitigated (Article 40(4) DSA). This makes systemic risks central to data access requests. The concept leaves room for a lot of interpretation. The DSA does not provide a clear definition, but shapes the meaning of systemic risks in Article 34(1). The article uses four *non-exhaustive* (Hofmann and Raue 2025) examples to illustrate systemic risks: (a) the dissemination of illegal content; (b) actual or foreseeable negative effects for the exercise of fundamental rights; (c) actual or foreseeable negative effects on civic discourse and electoral processes and public security; (d) actual or foreseeable negative effects in relation to gender-based violence, the protection of public health and serious negative consequences to the person's physical and mental well-being. In assessing these risks, online platforms can include contributing factors listed in the second paragraph of the article: (i) the design of their recommender system and other algorithmic systems; (ii) their content moderation systems; (iii) the applicable terms and conditions and their enforcement; (iv) systems for selecting and presenting advertisements; and (v) data related practices of the provider. The risks may also be influenced by intentional manipulation of the platform service, for example, through inauthentic use or the possible virality of illegal or harmful content content.

As systemic risks are so broad, this can create challenges for data access requests. For example, if a researcher was interested in studying recommender systems that amplify dissemination of hate speech (Weimann and Masri 2023), this can fall under the 'dissemination of illegal content' category since certain types of hate speech are illegal (Hietanen and Eddebo 2023).² However, hate speech can have negative effects on the exercise of fundamental rights, such as human dignity, private life, and non-discrimination, which are all well established in European Court of Human Rights case law.³ It can even have negative effects on civic discourse, elections, and public security.⁴ Moreover, hate speech can have serious consequences for gender-based violence and a person's mental well-being.⁵ It is therefore hard to cate-

²See also Council Framework Decision 2008/913/JHA of 28 November 2008 on combating certain forms and expressions of racism and xenophobia by means of criminal law; European Court of Human Rights, *Erbakan v Turkey*, para 56.

³See for instance European Court of Human Rights, *Lenis v Greece*, para 55; *Beizaras & Lecikas v Lithuania*, para 117; *Ivanov v Russia*.

⁴See for instance European Court of Human Rights, *Sanchez v France*.

⁵See for instance European Court of Human Rights *Beizaras & Lecikas v Lithuania*.

gorise the platform features leading to systemic risks. This represents an additional barrier in how researchers frame their data access requests.

Data Needed for Systemic Risks Research: Election Interference as a Case Study

Election interference has been one of the original smoking guns in terms of abusing social media architectures at scale to benefit private interests at the detriment of democratic processes. A well-known example in this respect is the Cambridge Analytica scandal (Meredith 2018), where private actors accessed Facebook data to profile and target voters in the United States 2016 presidential election and in the Brexit referendum (Cadwalladr and Graham-Harrison 2018). The vulnerabilities of social media platforms, particularly during elections, have also come to light in the recent Romanian presidential elections of 2024 (Luțac 2024).

We take this incident as a case study to concretely discuss what data could be requested and for what systemic risks under the DSA's data access regime for vetted researchers. This case study is important for at least two reasons. First, the Romanian situation is the first post-DSA election interference investigation by the European Commission (Commission 2024). This raises urgent practical questions such as what precisely needs to be studied in this context and, most importantly, what data is necessary to investigate systemic risks and mitigation strategies to illustrate what barriers researchers might face in requesting access to data under the DSA. Second, this case study contributes to existing scholarly debates around election interference, which have traditionally been US-centric or focused on Western Europe (Chong and McIntyre 2020; Unknown 2020), whereas Eastern Europe still maintains significant understudied post-communist complexities. To operationalise these implications for data access, we first outline the known features of the alleged Romanian election interference. Second, we introduce two factors that we argue lead to a systemic risk (platform manipulation and hidden advertising) and discuss them by extracting data needs from relevant research studies and further proposing specific computational research tasks as examples.

A Brief Overview of an Election Case Study

The Romanian presidential election campaign took place between October 25 and November 24, 2024. According to investigative journalists and Romanian intelligence agencies (Luțac 2024; Snoop.ro 2025; a României 2025), TikTok is the platform most heavily exploited to influence voters to support a right-wing candidate who went in a couple of weeks from being unknown to the most popular candidate in the voting results of the first voting round on November 24, 2024. The candidate's engagement relied on positive comments driving engagement and video views on TikTok. The amplified content included, among others, a combination of conspiracy theories, the rejection of Western interpretations of fundamental rights perceived as overly liberal, fascism, misogyny, and racism. This was also reflected by the artificial and later organic engagement involv-

ing this content (Snoop.ro 2025). Overall, the amplification also triggered TikTok's search recommendations, a feature unique to TikTok's increasing use as a search engine, to curate, deliver and further amplify content from and about the candidate. Suspecting manipulation and citing possible foreign state interference, Romania's Constitutional Court annulled the results of the first round of the presidential elections (a României 2024), and the European Court of Human Rights refused the candidate's request for an interim measure to suspend the Constitutional Court's decision (of Human Rights 2025).

Preliminary evidence (Luțac 2024; Snoop.ro 2025; a României 2025) points to the use of TikTok in the Romanian elections through a combination of: (i) **Inauthentic behaviour**: A coordinated network of direct promotion accounts generated fake engagement and triggered TikTok's search recommendations; (ii) **Political influencer marketing**: At least one non-disclosed micro-influencer campaign revolving around the promotion of an (unnamed) ideal candidate; and (iii) **Livestream gifting**: TikTok's streaming monetisation affordances (coins and gifts) were used to amplify (undisclosed) political advertising and political content.

This preliminary evidence is important in establishing a general narrative around how systemic risks might have been shaped in this election interference incident. However, investigative journalists can only analyse TikTok data externally by scraping it themselves or by relying on third-party tools (Luțac 2024), and intelligence agencies are not clear about how exactly they investigated the platform (a României 2025). DSA data access for academic researchers is thus an avenue to study systemic risks using scientific methodologies. Yet, in order to do so, researchers must first identify the actual systemic risks and the data they need to investigate.

The systemic risks surrounding the alleged interference in the Romanian presidential elections are multidimensional. The most obvious link in this case is to the election-related systemic risk. However, the other mentioned categories of systemic risks are also relevant: the dissemination of hidden advertising or hate speech (illegal content) (Article 34(1)(a)), the prevalence of hate speech as fundamental rights violations (Article 34(1)(b)), or the promotion of conspiracy theories affecting public health (Article 34(1)(d)) can also be systemic risks associated with the Romanian situation. In addition, these risks stem from a multitude of factors, as listed in Article 34(2), such as the design of TikTok's recommender system, its moderation systems, its policies regarding advertisements, or even the overall manipulation of the platform itself. In the context of this case study, we propose that in understanding the systemic risk of election interference in Romania, as mentioned in Article 34(1)(c), two factors are central: platform manipulation (Section) and hidden advertising (Section).

Platform Manipulation and Election Interference: Related Studies and Data Needs

Platform manipulation, as relevant to election manipulation, refers to the deliberate use of various social media platform

affordances to influence public opinion, behaviour, or perception, often including the use of deceptive and unethical means (Akhtar et al. 2024; Martino et al. 2020). This can involve the spread of false information on social media platforms (Vosoughi, Roy, and Aral 2018; Ferrara 2015), the use of automated accounts (bots) to amplify online content (Woolley 2016; Bessi and Ferrara 2016), and coordinated campaigns designed to mislead or sway public opinion (Zannettou et al. 2019a,b). It can also involve the deliberate manipulation of specific platform affordances such as recommendation algorithms in an attempt to amplify content favouring one perspective while suppressing content from another, usually conflicting viewpoint (Santos, Lelkes, and Levin 2021; Huszár et al. 2022). This section reviews some of the documented techniques used for trying to influence the outcome of elections with the objective of identifying the data necessary for empirical studies.

Identifying False Information During Elections. The spread of false information on social media platforms represents a significant and persistent challenge in the digital age (Zannettou et al. 2019c; Ferrara et al. 2020). The problem of false information arises from the ease with which online content can be created, shared, and amplified across a large number of users. False information, irrespective of whether intentional or unintentional, has the potential to influence public opinion and change voter behaviour, exacerbate online polarisation, and even affect the integrity of electoral processes.

In response to this issue, social media platforms employ content moderation strategies, encompassing diverse measures designed to remove false information, demote it, or leave it accessible while providing additional context to help users critically assess its veracity. For instance, during the 2020 US elections, Twitter employed warning labels to inform users about false information related to political narratives (Zannettou 2021).

Due to the potential impact of spreading misleading information, the research community has devoted significant resources to studying false information on social media platforms in various disciplines, with research focusing on exposure to untrustworthy websites (Guess, Nyhan, and Reifer 2020), analysing the spread of false information during elections and its impact on society (Allcott and Gentzkow 2017; Bovet and Makse 2019; Grinberg et al. 2019) and designing mitigation strategies like the use of fact-checking (Clayton et al. 2020), nudges (Pennycook et al. 2020) or warnings to end-users about the veracity of information (Zannettou 2021). Below, we summarise some notable work focusing on false information during elections and the data they used.

Allcott and Gentzkow (Allcott and Gentzkow 2017) studied false information on social media during the 2016 US elections. By combining web browsing data, user surveys, and data from fact-checkers, they empirically investigate the prevalence of false information during the 2016 US elections. This study used many diverse data fields: 1) *Content Data* (browsing histories), 2) *User Data* (from user surveys), 3) *Engagement Data* (how many times each real/fake article was shared), and 4) *Moderation-related Data* (i.e., whether the articles are determined as fake or real by fact checkers).

Grinberg et al. (Grinberg et al. 2019) studied the spread of fake news on Twitter and its connection with voter behaviour during the 2016 US presidential elections. The authors analysed public voter registration records on Twitter accounts, focusing on the exposure and spread of false information. The study used: 1) *Content Data* (tweets content), 2) *User Data* (Twitter account data), 3) *Network Data* (follower network on Twitter), and 4) *Temporal data* (fake news exposure over time). Bovet and Makse (Bovet and Makse 2019) studied the influence of false information on Twitter by analysing a large-space dataset of tweets that included links to news outlets during the 2016 US elections. By characterising the networks of information flows, they identified the most important influencers for sharing false information and their impact on the US elections. The study used: 1) *Content Data* (tweets content), 2) *User Data* (Twitter account data), and 3) *Network Data* (follower network on Twitter). Other research focused on analysing content moderation interventions on false information related to elections. Specifically, Zannettou (2021) studied the application of soft moderation interventions (i.e., warning labels) during the 2020 US elections, finding, among other things, that tweets with warning labels received more engagement than ones without. This work used the following data: 1) *Content Data* (tweets content), 2) *User Data* (Twitter account data), 3) *Moderation Data* (which tweets received warning labels), and 4) *Temporal Data* (Tweets with warning labels over time).

Identifying Coordinated Campaigns. Coordinated campaigns refer to organised efforts to amplify or push specific narratives on social media. The goals of these efforts vary from sowing public discord to achieving various political or commercial goals. Such campaigns usually employ multiple accounts that are operated by automated bots or humans to execute a unified strategy.

Coordinated campaigns often use automated accounts (bots). The detection of bots used for content amplification and algorithmic manipulation has been a significant research focus. The use of automated accounts requires the creation/purchasing of accounts that are posing as regular human accounts. These fake accounts are controlled by automated means and aim to assist in the spread or amplification of specific content. In many cases, such accounts are dormant for years and are activated for a particular purpose. The research community has studied automated accounts on social media during elections (Ferrara et al. 2020), focusing mainly on understanding their role and behaviour (Shao et al. 2018; Ferrara 2017) and assessing their impact (Bessi and Ferrara 2016; Eady et al. 2023).

Specifically, Shao et al. (Shao et al. 2018) analyse social bots and their role in sharing low-credibility content, finding that during the 2016 US elections, social bots shared a disproportionate amount of low-credibility content. To conduct their study, they used the following data: 1) *Content Data* (tweets), 2) *User data* (Twitter account information), 3) *Moderation Data* (news sources with low credibility information), and 4) *Engagement Data* (retweet information). Bessi and Ferrara (Bessi and Ferrara 2016) investigate how social bots affect political discussion during the 2016 US elections, finding that the presence of bots can negatively

affect political discussion on Twitter. To conduct their research, they relied on the following data: 1) *Content Data* (tweets), 2) *User Data* (Twitter account information), 3) *Temporal Data* (tweets over time), and 4) *Geospatial Data* (location of the tweets). The same kind of data was also applied by Ferrara (Ferrara 2017) to study social bots during the 2017 French election. Ferrara et al. (Ferrara et al. 2020) focus on the 2020 US elections and show that social bots online exacerbate the problem of political echo chambers. For their work, they used the following data: 1) *Content Data* (tweets), 2) *User Data* (Twitter account information), 3) *Temporal Data* (tweets over time), 4) *Moderation Data* (tweets shared by state-sponsored actors), and 5) *Engagement Data* (retweet information).

Another well-known implementation of such campaigns uses *state-sponsored trolls*, which are humans who operate a set of fake accounts, are sponsored by their governments, and aim to push specific narratives on social media to push their government's agenda. Examples include Russian trolls active on social media platforms during the 2016 US elections (Badawy, Ferrara, and Lerman 2018). Previous work on coordinated campaigns using state-sponsored trolls focused on analysing their characteristics and the strategies employed (Zannettou et al. 2019a), detecting actors involved in such campaigns during elections (Luceri, Giordano, and Ferrara 2020), and understanding their impact and influence on the Web and our society (Golovchenko et al. 2020; Badawy, Ferrara, and Lerman 2018). Specifically, Badawy et al. (Badawy, Ferrara, and Lerman 2018) investigate the Russian interference campaign on Twitter during the 2016 US presidential election. They analysed a large dataset of tweets to demystify the strategies used by the Internet Research Agency (IRA), a Russian organization known for its online propaganda, and analysed the Twitter users that engaged with tweets shared by IRA. The data used for this study include: 1) *Content Data* (tweets), 2) *User Data* (Twitter account information), 3) *Network Data* (retweet network), 4) *Moderation Data* (Accounts identified as IRA accounts), 5) *Temporal Data* (IRA tweets over time), 6) *Engagement Data* (people who engaged with IRA tweets), and 7) *Geospatial Data* (Location of tweet posting). Zannettou et al. (Zannettou et al. 2019a) analyse the behaviour and strategies employed by IRA trolls on Twitter during the 2016 US elections and assess the influence that they had on other platforms like 4chan and Reddit. This study leveraged the following data: 1) *Content Data* (tweets), 2) *User Data* (Twitter account information), 3) *Moderation Data* (Accounts identified as IRA accounts), 4) *Temporal Data* (IRA tweets over time), and 5) *Geospatial Data* (Location of tweet posting). Similarly, Golovchenko et al. (Golovchenko et al. 2020) investigated IRA's tweets during the 2016 US elections, focusing on analysing the YouTube videos included in IRA tweets. The data used for this study include: 1) Content data (tweets), 2) User data (Twitter account information), and 3) Moderation data (Accounts identified as IRA accounts). Other research efforts focused on detecting actors involved in such campaigns. An example is the work from Luceri et al. (Luceri, Giordano, and Ferrara 2020), which focused on detecting state-sponsored trolls that were involved in the

2016 US elections using an inverse reinforcement learning approach. To achieve this, they used the following data: 1) *Content Data* (tweets), 2) *User Data* (Twitter account information), and 3) *Moderation Data* (Accounts identified as IRA accounts).

Another method of recruiting user accounts for promoting the messages of a coordinated information campaign is employing social-media influencers. This strategy has been observed soon after Russia's invasion of Ukraine ("Russian lives matter" campaign (Richards 2022)) and has also been noted in the Romanian 2024 presidential elections (Popoviciu 2024). We discuss more on this strategy in the context of hidden advertising in Section .

Identifying Algorithmic Manipulation. Algorithmic manipulation refers to the intentional exploitation of platform algorithms and systems to amplify/suppress specific narratives or distort user engagement (Conti et al. 2024). Platform algorithms include recommendation systems (systems responsible for recommending content to users), algorithms for content search and ranking, and algorithms that identify trending topics based on user activity (Elmas et al. 2021). Nowadays, social media platforms increasingly rely on AI algorithms to enhance user experience, including recommendation systems to generate personalised feeds, recommend users to follow, etc. Given the increasing reliance of social media platforms on AI-based algorithms for recommending content to users, there are several concerns with respect to how such systems can be exploited by malicious actors that aim to manipulate the public and promote/suppress specific narratives online.

Motivated by this, previous research focused on understanding these phenomena. For instance, Conti et al. (Conti et al. 2024) conducted a quantitative study on suspicious changes in content visibility on Twitter, likely due to algorithmic interventions. To conduct their research, the authors used the following data: 1) *Content Data* (tweets), 2) *User Data* (Twitter account information), 3) *Algorithmic Data* (content visibility as determined by the algorithm), 4) *Temporal Data* (tweets over time), 5) *Engagement Data* (retweet information), and 6) *Moderation Data* (content factuality based on the sources). Another example of algorithmic manipulation was shown by Elmas et al. (Elmas et al. 2021), who demonstrated how the Twitter trending algorithm can be manipulated to promote specific political content in Turkey during the 2019 Istanbul elections. To demonstrate this kind of algorithmic manipulation, they used the following data: 1) *Content Data* (tweets), 2) *User Data* (Twitter account information), 3) *Algorithmic Data* (Trending topics), and 4) *Temporal Data* (algorithmic manipulation attacks over time).

Summary of Data Requirements. The overview below summarises the data points that could be relevant in the scientific investigation of platform manipulation based on prior literature and proposes examples of specific tasks which can use this data.

- **Content Data:** Text, images, videos, sound, transcriptions, hashtags, user mentions (Allcott and Gentzkow 2017; Grinberg et al. 2019; Zannettou 2021). *Example*

use case: Analyse and detect posts that share false information during elections.

- **User Data:** Account metadata, such as the account creation date, follower count, user demographics, bios, status, etc. *Example use case*: Study the personas of accounts pertaining to state-sponsored actors (Badawy, Ferrara, and Lerman 2018; Zannettou et al. 2019a; Luceri, Giordano, and Ferrara 2020).
- **Engagement Data:** Metrics such as likes, shares, comments, and views (Allcott and Gentzkow 2017; Bovet and Makse 2019; Zannettou 2021). *Example use case*: Analysing user engagement with false information related to elections.
- **Moderation Data:** Posts or content flagged, removed, or labelled by the platform or external sources (e.g., fact-checkers) (Badawy, Ferrara, and Lerman 2018; Luceri, Giordano, and Ferrara 2020; Zannettou et al. 2019a; Ferrara et al. 2020; Shao et al. 2018). Also, moderation data on the user level, e.g. whether a user account is suspected to be a bot or controlled by a state-sponsored actor. *Example use case*: Studying the effectiveness of platform moderation interventions for posts sharing false information.
- **Temporal Data:** Time-based activity logs, such as the engagement that a misinformation record receives over time (Grinberg et al. 2019; Zannettou 2021; Conti et al. 2024). *Example use case*: Analysing a timeline of the dissemination of a false narrative before an election.
- **Network Data:** Data about the social graph, such as user connections and interactions. *Example use case*: Analysing influential nodes in disseminating false information (Grinberg et al. 2019; Badawy, Ferrara, and Lerman 2018).
- **Algorithmic Data:** Data on algorithmic outputs and decisions (e.g., videos recommended to end-users), as well as the importance of various features in algorithmic outputs (Elmas et al. 2021; Conti et al. 2024). *Example use case*: Investigating changes in content visibility due to algorithmic manipulation.
- **Geospatial Data:** Anonymised and aggregate location data (Badawy, Ferrara, and Lerman 2018; Zannettou et al. 2019a; Bessi and Ferrara 2016; Ferrara 2017). *Example use case*: Identifying and analysing coordinated campaigns originating from specific regions.

Political Influencer Marketing as Hidden Advertising

The popularity of influencer marketing has been growing steadily from US\$35.1bn in 2024 to US\$52bn expected in 2028 (Statista 2024). Its advantages, particularly the opportunity to embed advertising with organic content made by creators who establish parasocial relationships with their followers, make it an incredibly compelling marketing strategy – even for political advertising. Candidates and political entities find it important to partake in the creator economy, and creators themselves are pressured to make more political content and engage with social justice questions (Siu 2024).

Measuring the Prevalence of Undisclosed Ads. Undisclosed advertisements have been widely acknowledged as a major regulatory concern by various legislative bodies, including the European Commission (EC) drafting the DSA (Duijvenvoorde and Goanta 2023). Enforcement of the DSA in the realm of political advertising is of great significance since it could safeguard the free expression of diverse political ideologies and help maintain democratic integrity. In the context of the Romanian elections, political ideologies were disseminated through seemingly credible media channels, including social media influencers. When political advertising is not disclosed, audiences are less likely to recognise the content as advertisements (or other paid arrangements), leaving them vulnerable to manipulation (Liu, Yu, and Yang 2024). This lack of transparency allows certain political candidates to exploit misinformation and covert persuasion tactics, potentially swaying voter behaviour and gaining an unfair electoral advantage. Such practices not only undermine voter autonomy but also jeopardise the legitimacy of democratic processes. This issue aligns with broader concerns regarding systemic risks posed by hidden advertising as illegal content. Measuring the prevalence of hidden political advertisements is, therefore, a critical step in establishing whether they are a factor in the understanding of election-related systemic risks. By assessing how frequently and in what forms undisclosed political ads appear, regulators can gain valuable insights into the scope of the problem. This, in turn, can inform the development of targeted interventions to ensure elections remain fair, transparent, and free from manipulation, thereby upholding democratic values and fostering trust in political elections.

Measuring the prevalence of undisclosed ads first requires identifying which posts contain sponsored content. Existing sponsored content detection research has primarily focused on commercial content, framing the problem as a machine learning classification task. Many models adopt a semi-supervised approach, using disclosure hashtags or keywords (e.g., #ad, #sponsored) as weak labels to distinguish between sponsored and organic posts (Kim, Jiang, and Wang 2021; Bertaglia et al. 2023). Studies rely primarily on *Content Data* (such as post captions, engagement metrics, and associated metadata) to train models (Zarei et al. 2020; Bertaglia et al. 2023, 2025). Kim, Jiang, and Wang (2021) incorporate *Network Data* to model the relationship between influencers, brands, and (sponsored) posts and add more context to the machine learning models. Such approaches require additional *User Data*, including account metadata (e.g., follower counts, account type). Other studies combine image and text data to improve model performance (Sánchez Villegas, Goanta, and Aletras 2023; Villegas, Mokaram, and Aletras 2021). In this context, such multimodal models would benefit from additional *Content Data*, including attributes inferred by the platforms (e.g., detected objects in videos, audio transcriptions, and visual markers of sponsorship).

Beyond detecting undisclosed ads, measuring their prevalence at scale requires additional data, particularly about influencer accounts and their activity. For our election case study, researchers would need access to *User Data* to identify political influencers, including lists of influencers,

demographic attributes, account metadata (e.g., follower counts), and account types. *Content Data*, such as text, images, videos, and inferred attributes (e.g. object detection) from influencer posts would be essential to detect undisclosed ads. *Engagement Data*, including likes, shares, comments, and views, would help analyse implication patterns and detect coordinated behaviour. *Network Data* would be important to map connections between influencers, political actors, and audience interactions. Finally, *Moderation Data*, such as platform-inferred labels or flags related to sponsored or political content, could indicate existing detection mechanisms.

Measuring the Engagement of Organic Content, Disclosed and Undisclosed Ads. A key reason behind the non-disclosure of advertisements is the widespread belief that revealing sponsorships harms audience engagement. Influencers, who simultaneously act as content creators and advertising platforms, grapple with the tension between protecting their long-term growth and maximising short-term profits. The assumption that disclosure reduces engagement incentivises some influencers to conceal sponsorships. Understanding the actual impact of advertisements and their (non)disclosure on engagement is therefore crucial for assessing the validity of this belief. Empirical studies have analysed the effects of disclosures and regulations on engagement, relying on *Engagement Data* to compare audience reactions to disclosed versus undisclosed ads, as well as before and after specific regulations (Ershov and Mitchell 2020; Bertaglia et al. 2025). However, effectively measuring these differences requires a longitudinal perspective; therefore, *Temporal Data*, especially in the form of engagement metrics over time, is essential for understanding the persistence and impact of undisclosed advertising. Research can be designed to compare engagement levels across organic content and disclosed and undisclosed advertisements. If empirical findings refute the assumption that disclosure negatively affects engagement, this could pave the way for educational initiatives aimed at influencers, emphasising that transparency does not undermine engagement. Such efforts could, in turn, improve compliance rates with disclosure regulations.

Assessing How Platforms Promote or Moderate Sponsored Content. Another reason for the non-disclosure of advertisements stems from a belief among influencers that platforms deliberately restrict the visibility of advertising content (Musiyiwa and Jacobson 2023; Savolainen 2022; Bishop 2019). This perception is linked to the inherent tension platforms face between increasing user traffic and maximising financial gains. While displaying more ads aligns with the interests of advertisers, it risks alienating users and discouraging them from engaging with the platform. Consequently, platforms are compelled to strike a balance between promoting and moderating advertisements to sustain their ecosystem. Due to this concern, an ideal choice for the influencers would be to hide the advertisement so that they can bypass the moderation process. To address this issue, it is crucial to understand how platforms' content promotion and moderation mechanisms operate. Research could explore the factors influencing the visibility of advertising content, such

as algorithmic preferences, user behaviour data and the balance between paid and organic content. By examining the biases inherent in these systems, such research could identify patterns that favour or limit certain types of content, providing valuable insights into how platforms manage the promotion and visibility of advertisements. In practice, investigating whether and how platforms moderate or amplify advertising content requires access to several key data types. In addition to the data points identified for the previous tasks, *Algorithmic Data*, such as content recommended to users and features related to their ranking, would be essential for determining how sponsored content performs in the recommender system within the platform.

Summary of Data Requirements. The overview below summarises the data points that could be relevant in the scientific investigation of hidden advertising based on prior literature and proposes examples of specific tasks for the analysis of this data.

- **Content Data:** All media content (text, images, videos, and sound), metadata (e.g., captions, timestamps, and hashtags), and inferred attributes (e.g., object detection and visual sponsorship markers) from influencer posts. These data points are fundamental for identifying advertising content (Zarei et al. 2020; Bertaglia et al. 2023; Villegas, Mokaram, and Aletras 2021; Sánchez Villegas, Goanta, and Aletras 2023). *Example use case:* Training machine learning models to detect undisclosed political ads.
- **User Data:** Metadata related to influencer accounts, including follower counts, account creation date, account type, and inferred demographics. Studying influencer engaging in political campaigns requires access to lists of content creators and their attributes (Kim, Jiang, and Wang 2021; Bertaglia et al. 2025). *Example use case:* Mapping Romanian influencers involved in political campaigns by analysing account demographics and activity.
- **Engagement Data:** Metrics such as likes, shares, comments, and views across influencer posts (Ershov and Mitchell 2020). *Example use case:* Analysing the impact of disclosures and regulation in engagement with political posts.
- **Moderation Data:** Information on platform-inferred labels, content flagging, removals, and downranking of sponsored and political content. This data would help determine whether automated moderation disproportionately affects disclosed versus undisclosed ads (Musiyiwa and Jacobson 2023; Savolainen 2022). *Example use case:* Assessing whether platform moderation algorithms label disclosed political ads differently from undisclosed ones.
- **Temporal Data:** Engagement metrics over time (Ershov and Mitchell 2020; Bertaglia et al. 2025). *Example use case:* Identify potential coordinated engagement with political content.
- **Network Data:** Interaction data capturing connections between influencers, brands, political entities, and audience members. Mapping these relationships helps detect coordinated campaigns and assessing the diffusion

of undisclosed ads (Kim, Jiang, and Wang 2021). *Example use case*: Detecting coordinated influence operations by analysing how content spreads across influencer networks.

- **Algorithmic Data**: Includes recommendation system outputs, ranking metrics, and visibility logs for influencer content. Access to this data is essential to assess whether platform recommendation systems amplify or suppress disclosed advertisements compared to undisclosed content (Savolainen 2022). *Example use case*: Analysing whether recommendation algorithms rank disclosed political ads differently from undisclosed ones.

Data Availability as a Platform Governance Narrative

So far, we have focused on understanding what data would ideally be used to identify systemic risks. Knowing what data platforms have is essential for researchers to request data through Article 40 DSA. In their data access application under Article 8(6) DA, researchers are required to provide “an explanation as to why the research project cannot be carried out with alternative existing means such as using data available through other sources” – an incentive for researchers not to overburden the data access framework. Therefore, the researcher needs to show that the data they need are not publicly available (e.g. in a research API). In addition, to improve their chances of getting their data access applications through, researchers should also ensure that the data they seek is actually internally available with platforms. How platforms collect, process and store personal data from users in exchange for access to platform services can be inferred in two ways: (i) through *platform documentation* on user-facing webpages constituting the contractual relationship between users and the platform; and (ii) through *visible data* in APIs and user-requested data (data donations). In this section, we analyse TikTok’s documentation, its Research API, and data donations to identify discrepancies between what the platform says it collects and what it visibly collects. We then use this framework to analyse the gaps in the data needed to investigate platform manipulation and hidden advertising in the context of election interference, as outlined in the overviews of Sections 3.2 and 3.3.

In TikTok’s Privacy Centre,⁶ users can find a list of examples of “information that we *may* collect” (emphasis added) and, in the Safety Centre,⁷ a more detailed list of “some” of what is collected. Both user-facing webpages direct users to the Privacy Policy.⁸ While this addresses personal data collected from users, the TikTok Partner Privacy Policy covers information processed in relation to partner platforms that include TikTok for Business, TikTok Shop and TikTok Creator Marketplace.

We focus on the user-facing Privacy Policy, which outlines “what information we collect”, organised by three types: “information you provide”, “automatically collected

information”, and “information from other sources”. Under each category, the policy lists different types of information with specific data included as examples. While the nature of platform development necessitates flexibility in the policy, and users can understand categories of data, definitive data points only emerge in “such as” lists, impeding clarity of what data platforms have. For example, TikTok states, “We infer your attributes (such as age-range and gender) and interests based on the information we have about you” indicating the non-exhaustive nature of the wording.

Drawing on the data mentioned in this Privacy Policy, we evaluate the availability of data requirements described in the case study. We find that not all the data required for studying the identified systemic risks are included. We then turn to other platform documentation, such as the *Branded Content Policy*⁹ and *Help Pages*,¹⁰ to ascertain whether this is data that TikTok processes and so could be requested. For instance, algorithmic parameters and recommended search terms are generated by the platform and are not personal data that would need to be described in the privacy policy. Table 1 lists the documentation source for each data point relevant to the case study.

We then determine whether each data point is available through the Research API or data donations. The latter was obtained by the authors from their own TikTok research accounts. The API provides qualifying research access to certain public data, while data donations (Van Driel et al. 2021; Zannettou et al. 2023) provide individual users with their personal data, which can then be donated to researchers. While other approaches, such as web scraping, are used for research purposes, we focus on these two mechanisms that comply with the terms of service of the platform and so would render a data access request through Article 40 unnecessary.

Using TikTok documentation for the API and data donations, which detail the exact data points available, we ensure that the form in which they are provided would be sufficient for the needs identified in the scenarios. We classify the availability of each data point as *available*, *not available*, or *limited*. For example, we identify *Comment* data and *FYP history* as limited: the Research API limits the collection of comments to the top 1000 and does not specify what constitutes “top”. Similarly, although viewing history is available through data donations, it includes not only content recommended to the user through the *For You Page*, but also content viewed through other sources such as direct messages or the follower feed. Figure 1 illustrates the distribution of data availability. Each coloured circle represents a data point nested within a circle area showing the higher-level data category. The colours signify the level of availability; we consider the API as the most effective mechanism for data collection in our scenarios. For data donations, we would require access to either the accounts posting the election-related content or the users viewing such content, which are populations challenging to identify and recruit.

Our analysis demonstrates that the existing mechanisms

⁶<https://www.tiktok.com/privacy/overview/en>.

⁷<https://www.tiktok.com/safety/en/>.

⁸<https://www.tiktok.com/legal/page/eea/privacy-policy/en>.

⁹<https://www.tiktok.com/legal/page/global/bc-policy/en>.

¹⁰<https://support.tiktok.com/en/>.

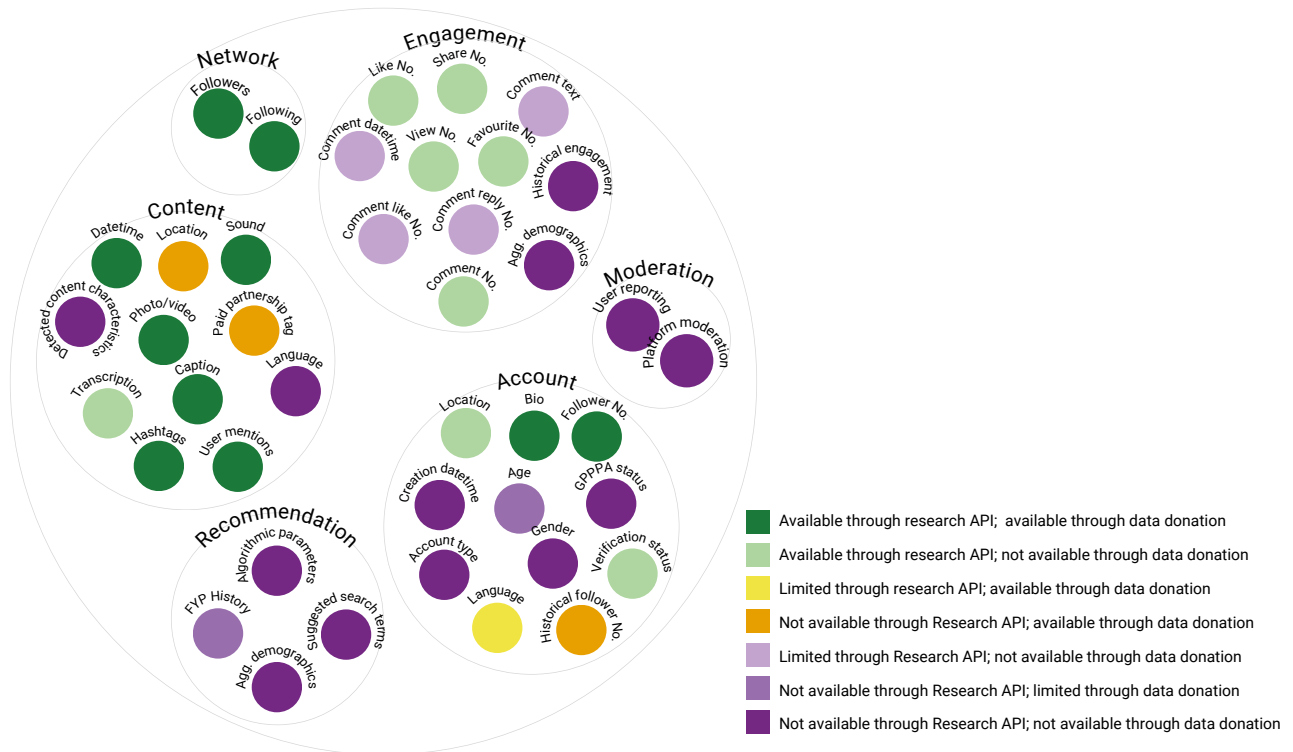


Figure 1: Availability of TikTok data for studying systemic risks in Romanian election interference incidents under existing access mechanisms, classified by data type and access method. Nested circles represent data categories with individual data points inside. Colours indicate accessibility, ranging from green (fully available via the Research API or data donations) to purple (entirely inaccessible to researchers), with intermediate shades representing partial access. The analysis highlights critical gaps in access, particularly in user attributes, algorithmic recommendations, and content moderation decisions, which limit researchers' ability to investigate the systemic risks described in our scenarios.

for data access provide insufficient means to investigate the systemic risks described in our case study. Not only can we not access any data related to *Recommendation* and *Moderation*, but also, even in the categories in which some data are available, the other necessary corresponding data points are not, such as accounts' attributed demographics and account type, thereby rendering the research questions unanswerable. Problematically, inferred attributes about content and user demographics cannot be accessed, impeding our ability to contextualise data and understand targeting and recommendation practices. Therefore, researchers are left with a limited perspective that detaches content and engagement from the people targeted by coordinated campaigns.

Conclusion: Reflections on DSA Data Access for the Research Community

The implementation of DSA Article 40 is a significant milestone in the pursuit of greater platform transparency and accountability. By granting vetted researchers access to data, this mechanism has great potential to uncover systemic risks and to foster a more informed regulatory landscape. However, our analysis reveals critical legal interpretational and operational challenges that hinder the realisation of this potential, due to how bureaucratic and cumbersome Article 40 will prove to be in practice. Not only are systemic risks very vague to define and identify, but requesting data can lead to a standoff problem between platforms and researchers. In the information asymmetry defining digital industries such as social media, not having a general overview of the data availability might hurt researchers' chances of getting data access, either because the requested data may be public in one way or another, or because the data are invisible, and platforms may deny having them.

Our case study of the Romanian election interference highlights the complexity of defining and operationalising systemic risks under the DSA (Article 34(1)(c)). This case study reveals how two election-related systemic risk factors—platform manipulation and hidden advertising—ought to be studied and what data is needed for such scientific investigations based on established literature in the relevant computational fields. In our account of data requirements for investigating systemic risk in the case study, we establish that current mechanisms provide researchers with insufficient access to data, necessitating access through Article 40. To do this, we relied on terms of service and other platform documentation to justify the availability of requested data, providing evidence that TikTok gathers, infers, and processes specified data to counteract the issue of opacity in knowing what data exists. While we propose and demonstrate how this exercise can be effective for researchers in preparing applications, the issue of transparency persists, particularly concerning what invisible data TikTok may collect. But how platforms will indicate what data and data structures are available, and the extent to which this will capture the totality of data available to researchers, raises questions about how DSCs and the European Commission will further operationalise this provision to address the standoff referred to above. This is all the more relevant

for cross-platform research, as our case study was limited to TikTok, but election interference is always prevalent beyond just one platform.

To address these challenges, we propose several general recommendations. First, clearer definitions and guidelines regarding the interpretation of systemic risks are essential to support researchers in framing their data requests effectively, particularly when national interpretations by DSCs can differ significantly. Second, improving transparency about the data platforms collect, infer, and process is crucial for resolving any ambiguity of researchers around data availability. Data inventories (Article 6(4) DA) provided by platforms could be a step in the right direction. The negotiation of what data should be mapped in such inventories could be further informed by additional case studies like the one discussed in this paper, which could identify, for different categories, the data gaps in publicly available or visible data. Finally, fostering collaboration between researchers, regulatory bodies, and platforms is necessary to ensure that the data access framework aligns with both academic and societal needs. The European Commission can play an important role in mediating exchanges of needs and interests to align expectations and ensure compliance with the transparency policy goals pursued by the DSA's data access regime.

References

- a României, A. P. 2025. Comunicat de presă. Accessed: 2025-01-22.
- a României, C. C. 2024. Comunicat de presă – 2 decembrie 2024. Accessed: 2025-01-22.
- Akhtar, M. M.; Masood, R.; Ikram, M.; and Kanhere, S. S. 2024. SoK: False Information, Bots and Malicious Campaigns: Demystifying Elements of Social Media Manipulations. In *Proceedings of the 19th ACM Asia Conference on Computer and Communications Security*, 1784–1800.
- Allcott, H.; and Gentzkow, M. 2017. Social media and fake news in the 2016 election. *Journal of economic perspectives*, 31(2): 211–236.
- Badawy, A.; Ferrara, E.; and Lerman, K. 2018. Analyzing the digital traces of political manipulation: The 2016 Russian interference Twitter campaign. In *2018 IEEE/ACM international conference on advances in social networks analysis and mining (ASONAM)*, 258–265. IEEE.
- Bertaglia, T.; Goanta, C.; Spanakis, G.; and Iamnitchi, A. 2025. Influencer self-disclosure practices on Instagram: A multi-country longitudinal study. *Online Social Networks and Media*, 45: 100298.
- Bertaglia, T.; Huber, S.; Goanta, C.; Spanakis, G.; and Iamnitchi, A. 2023. Closing the Loop: Testing ChatGPT to Generate Model Explanations to Improve Human Labelling of Sponsored Content on Social Media. In Longo, L., ed., *Explainable Artificial Intelligence*, 198–213. Springer Nature Switzerland.
- Bessi, A.; and Ferrara, E. 2016. Social bots distort the 2016 US Presidential election online discussion. *First monday*, 21(11-7).

- Bishop, S. 2019. Managing visibility on YouTube through algorithmic gossip. *New media & society*, 21(11-12): 2589–2606.
- Bovet, A.; and Makse, H. A. 2019. Influence of fake news in Twitter during the 2016 US presidential election. *Nature communications*, 10(1): 7.
- Cadwalladr, C.; and Graham-Harrison, E. 2018. Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach. Accessed: 2025-01-22.
- Chong, D.; and McIntyre, E. H. 2020. The Impact of COVID-19 on the Music Industry: A Study of the UK and US Markets. *Music Business Research*, 5(1): 27–40. Accessed: 2025-01-22.
- Clayton, K.; Blair, S.; Busam, J. A.; Forstner, S.; Gance, J.; Green, G.; Kawata, A.; Kovvuri, A.; Martin, J.; Morgan, E.; et al. 2020. Real solutions for fake news? Measuring the effectiveness of general warnings and fact-check tags in reducing belief in false stories on social media. *Political behavior*, 42: 1073–1095.
- Commission, E. 2024. Press release: [Title of the Press Release]. Accessed: 2025-01-22.
- Conti, M.; De Cristofaro, E.; Galeazzi, A.; Paudel, P.; and Stringhini, G. 2024. Revealing The Secret Power: How Algorithms Can Influence Content Visibility on Social Media. *arXiv preprint arXiv:2410.17390*.
- Duivenvoorde, B.; and Goanta, C. 2023. The regulation of digital advertising under the DSA: A critical assessment. *Computer Law & Security Review*, 51: 105870.
- Eady, G.; Paskhalis, T.; Zilinsky, J.; Bonneau, R.; Nagler, J.; and Tucker, J. A. 2023. Exposure to the Russian Internet Research Agency foreign influence campaign on Twitter in the 2016 US election and its relationship to attitudes and voting behavior. *Nature communications*, 14(1): 62.
- Elmas, T.; Overdorf, R.; Özkalay, A. F.; and Aberer, K. 2021. Ephemeral astroturfing attacks: The case of fake twitter trends. In *2021 IEEE European symposium on security and privacy (EuroS&P)*, 403–422. IEEE.
- Ershov, D.; and Mitchell, M. 2020. The Effects of Influencer Advertising Disclosure Regulations: Evidence From Instagram. In *Proceedings of the 21st ACM Conference on Economics and Computation*, EC '20, 73–74. Association for Computing Machinery.
- Ferrara, E. 2015. Manipulation and abuse on social media. *ACM SIGWEB Newsletter*, 2015(Spring): 1–9.
- Ferrara, E. 2017. Disinformation and social bot operations in the run up to the 2017 French presidential election. *arXiv preprint arXiv:1707.00086*.
- Ferrara, E.; Chang, H.; Chen, E.; Muric, G.; and Patel, J. 2020. Characterizing social media manipulation in the 2020 US presidential election. *First Monday*.
- Golovchenko, Y.; Buntain, C.; Eady, G.; Brown, M. A.; and Tucker, J. A. 2020. Cross-platform state propaganda: Russian trolls on twitter and YouTube during the 2016 US Presidential Election. *The International Journal of Press/Politics*, 25(3): 357–389.
- Grinberg, N.; Joseph, K.; Friedland, L.; Swire-Thompson, B.; and Lazer, D. 2019. Fake news on Twitter during the 2016 US presidential election. *Science*, 363(6425): 374–378.
- Guess, A. M.; Nyhan, B.; and Reifler, J. 2020. Exposure to untrustworthy websites in the 2016 US election. *Nature human behaviour*, 4(5): 472–480.
- Hietanen, M.; and Eddebo, J. 2023. Towards a Definition of Hate Speech—With a Focus on Online Contexts. *Journal of Communication Inquiry*, 47(4): 440–458. Publisher: SAGE Publications Inc.
- Hofmann, F.; and Raue, B., eds. 2025. *Digital Services Act: Article-by-Article commentary*. Nomos, first edition edition.
- Huszár, F.; Ktena, S. I.; O'Brien, C.; Belli, L.; Schlaikjer, A.; and Hardt, M. 2022. Algorithmic amplification of politics on Twitter. *Proceedings of the National Academy of Sciences*, 119(1): e2025334119.
- Kaushal, R.; Van De Kerkhof, J.; Goanta, C.; Spanakis, G.; and Iamnitchi, A. 2024. Automated Transparency: A Legal and Empirical Analysis of the Digital Services Act Transparency Database. In *The 2024 ACM Conference on Fairness, Accountability, and Transparency*, 1121–1132. ACM.
- Kim, S.; Jiang, J.-Y.; and Wang, W. 2021. Discovering Undisclosed Paid Partnership on Social Media via Aspect-Attentive Sponsored Post Learning. In *Proceedings of the 14th ACM International Conference on Web Search and Data Mining*, WSDM '21, 319–327. Association for Computing Machinery.
- Kosta, E.; and Brewczyńska, M. 2019. Government Access to User Data: Towards More Meaningful Transparency Reports. In Ballardini, R.-M.; and Pitkänen, O., eds., *Regulating Industrial Internet through IPR, Data Protection and Competition Law*, 253–274. Kluwer Law International.
- Leerssen, P. 2023. An end to shadow banning? Transparency rights in the Digital Services Act between content moderation and curation. *Computer Law & Security Review*, 48: 105790.
- Leerssen, P. 2024. Outside the Black Box: From Algorithmic Transparency to Platform Observability in the Digital Services Act. *Weizenbaum Journal of the Digital Society*, 4(2). Number: 2.
- Liu, Q.; Yu, S.-K.; and Yang, Y. 2024. The effects of sponsorship disclosure in short-form video: A moderated mediation model of sponsorship literacy and perceived features of sponsored short-form video. *Computers in Human Behavior*, 150: 107969.
- Luceri, L.; Giordano, S.; and Ferrara, E. 2020. Detecting troll behavior via inverse reinforcement learning: A case study of russian trolls in the 2016 us election. In *Proceedings of the international AAAI conference on web and social media*, volume 14, 417–427.
- Luțac, R. 2024. Rețeta boților lui Călin Georgescu: cum a obținut 4,5 milioane de vizualizări într-o zi pe un cont nou. *Snoop*. Accessed: 2025-01-22.
- Martino, G. D. S.; Cresci, S.; Barrón-Cedeño, A.; Yu, S.; Di Pietro, R.; and Nakov, P. 2020. A survey

- on computational propaganda detection. *arXiv preprint arXiv:2007.08024*.
- Meredith, S. 2018. Facebook-Cambridge Analytica: A timeline of the data hijacking scandal. *CNBC*. Accessed: 2025-01-20.
- Musiyiwa, R.; and Jacobson, J. 2023. Sponsorship disclosure in social media influencer marketing: The algorithmic and non-algorithmic barriers. *Social Media+ Society*, 9(3): 20563051231196870.
- of Human Rights, E. C. 2025. HUDOC Press Release. Accessed: 2025-01-22.
- Pasquale, F. 2016. *The Black Box Society: the Secret Algorithms that Control Money and Information*. Harvard University Press, first harvard university press paperback edition.
- Pennycook, G.; McPhetres, J.; Zhang, Y.; Lu, J. G.; and Rand, D. G. 2020. Fighting COVID-19 misinformation on social media: Experimental evidence for a scalable accuracy-nudge intervention. *Psychological science*, 31(7): 770–780.
- Popoviciu, A. 2024. TikTok influencers flee Romania amid tax probe into their election role. *Politico*. Accessed: 2025-01-22.
- Richards, A. 2022. A pro-Russia propaganda campaign is using over 180 TikTok influencers to promote the invasion of Ukraine. *Media Matters for America*. Accessed: 2025-01-22.
- Ross, T.; and Popoviciu, A. 2024. How Putin won the Romanian election. *Politico*. Accessed: 2025-01-20.
- Sánchez Villegas, D.; Goanta, C.; and Aletras, N. 2023. A Multimodal Analysis of Influencer Content on Twitter. In Park, J. C.; Arase, Y.; Hu, B.; Lu, W.; Wijaya, D.; Purwaranti, A.; and Krisnadhi, A. A., eds., *Proceedings of the 13th International Joint Conference on Natural Language Processing and the 3rd Conference of the Asia-Pacific Chapter of the Association for Computational Linguistics (Volume 1: Long Papers)*, 225–240. Association for Computational Linguistics.
- Santos, F. P.; Lelkes, Y.; and Levin, S. A. 2021. Link recommendation algorithms and dynamics of polarization in online social networks. *Proceedings of the National Academy of Sciences*, 118(50): e2102141118.
- Savolainen, L. 2022. The shadow banning controversy: perceived governance and algorithmic folklore. *Media, Culture & Society*, 44(6): 1091–1109.
- Shao, C.; Ciampaglia, G. L.; Varol, O.; Yang, K.-C.; Flammini, A.; and Menczer, F. 2018. The spread of low-credibility content by social bots. *Nature communications*, 9(1): 1–9.
- Siu, A. 2024. How the elections are shaping influencer marketing, from brand strategies to social media spending - Digiday.
- Snoop.ro. 2025. Campania PNL de pe TikTok ajunsă să-l sustină pe Georgescu a fost ideea lui Rareș Bogdan: “Am știut, dar de online nu m-am ocupat eu”. Accessed: 2025-01-22.
- Statista. 2024. Influencer Advertising - Global | Statista Market Forecast.
- Unknown, A. 2020. Title Unknown. *The Electrochemical Society Journal*, 68(3): 1234–1245. Accessed: 2025-01-22.
- Urman, A.; and Makhortykh, M. 2023. How transparent are transparency reports? Comparative analysis of transparency reporting across online platforms. *Telecommunications Policy*, 47(3): 102477.
- Van Driel, I.; Giachanou, A.; Pouwels, J. L.; Boeschoten, L.; Beyens, I.; Valkenburg, P. M.; et al. 2021. Promises and pitfalls of Instagram data donations. *OSFPREPRINTS*.
- Villegas, D. S.; Mokaram, S.; and Aletras, N. 2021. Analyzing Online Political Advertisements. In *Findings of the Association for Computational Linguistics: ACL-IJCNLP 2021*, 3669–3680.
- Vosoughi, S.; Roy, D.; and Aral, S. 2018. The spread of true and false news online. *science*, 359(6380): 1146–1151.
- Weimann, G.; and Masri, N. 2023. Research Note: Spreading Hate on TikTok. *Studies in Conflict & Terrorism*, 46(5): 752–765. Publisher: Routledge eprint: <https://doi.org/10.1080/1057610X.2020.1780027>.
- Woolley, S. C. 2016. Automating power: Social bot interference in global politics. *First Monday*.
- Zannettou, S. 2021. “I Won the Election!”: an empirical analysis of soft moderation interventions on Twitter. In *Proceedings of the international AAAI conference on web and social media*, volume 15, 865–876.
- Zannettou, S.; Caulfield, T.; De Cristofaro, E.; Sirivianos, M.; Stringhini, G.; and Blackburn, J. 2019a. Disinformation warfare: Understanding state-sponsored trolls on Twitter and their influence on the web. In *Companion proceedings of the 2019 world wide web conference*, 218–226.
- Zannettou, S.; Caulfield, T.; Setzer, W.; Sirivianos, M.; Stringhini, G.; and Blackburn, J. 2019b. Who let the trolls out? towards understanding state-sponsored trolls. In *Proceedings of the 10th acm conference on web science*, 353–362.
- Zannettou, S.; Nemeth, O.-N.; Ayalon, O.; Goetzen, A.; Gummadi, K.; Redmiles, E. M.; and Roesner, F. 2023. Leveraging rights of data subjects for social media analysis: Studying TikTok via data donations. *arXiv preprint arXiv:2301.04945*.
- Zannettou, S.; Sirivianos, M.; Blackburn, J.; and Kourtellis, N. 2019c. The web of false information: Rumors, fake news, hoaxes, clickbait, and various other shenanigans. *Journal of Data and Information Quality (JDIQ)*, 11(3): 1–37.
- Zarei, K.; Ibosiola, D.; Farahbakhsh, R.; Gilani, Z.; Garimella, K.; Crespi, N.; and Tyson, G. 2020. Characterising and Detecting Sponsored Influencer Posts on Instagram. *arXiv:2011.05757 [cs]*.

Paper Checklist

1. For most authors...
 - (a) Would answering this research question advance science without violating social contracts, such as violating privacy norms, perpetuating unfair profiling, exacerbating the socio-economic divide, or implying disrespect to societies or cultures? **Yes. This is a conceptual paper that analyses the DSA's Article 40 data-access mechanism and, via a case study, specifies what kinds of data would be needed to study systemic risks. We do not collect, process, or publish personal data, nor do we scrape platforms or build models that profile individuals or groups.**
 - (b) Do your main claims in the abstract and introduction accurately reflect the paper's contributions and scope? **Yes. The abstract and introduction accurately state our contributions.**
 - (c) Do you clarify how the proposed methodological approach is appropriate for the claims made? **Yes. We clarify that this is a conceptual and methodological paper: we derive data needs from prior literature on systemic risks, map them onto the Romanian election case study, and compare these needs with what TikTok documentation, the Research API, and data donations provide. This approach is appropriate for the claims we make, as our contribution is to outline methodological requirements and gaps, not to produce new empirical findings.**
 - (d) Do you clarify what are possible artifacts in the data used, given population-specific distributions? **NA. This paper does not use empirical datasets.**
 - (e) Did you describe the limitations of your work? **Yes. We discuss the limitations of our work, including the interpretational uncertainty of systemic risks under the DSA, the lack of transparency about what data platforms actually collect, and the insufficiency of currently available mechanisms (APIs and data donations) to study election-related systemic risks. We also acknowledge that our case study focuses only on TikTok, not covering the cross-platform nature of systemic risks.**
 - (f) Did you discuss any potential negative societal impacts of your work? **NA. As a conceptual paper, we do not conduct empirical analysis or release tools or datasets that could have direct negative societal impacts.**
 - (g) Did you discuss any potential misuse of your work? **NA. The paper does not produce datasets, tools, or empirical models that could be misused. Our contribution is limited to conceptual analysis and a case study framing of data needs under the DSA.**
 - (h) Did you describe steps taken to prevent or mitigate potential negative outcomes of the research, such as data and model documentation, data anonymization, responsible release, access control, and the reproducibility of findings? **NA.**
 - (i) Have you read the ethics review guidelines and ensured that your paper conforms to them? **Yes.**
2. Additionally, if your study involves hypotheses testing...
 - (a) Did you clearly state the assumptions underlying all theoretical results? **NA.**
 - (b) Have you provided justifications for all theoretical results? **NA.**
 - (c) Did you discuss competing hypotheses or theories that might challenge or complement your theoretical results? **NA.**
 - (d) Have you considered alternative mechanisms or explanations that might account for the same outcomes observed in your study? **NA.**
 - (e) Did you address potential biases or limitations in your theoretical framework? **NA.**
 - (f) Have you related your theoretical results to the existing literature in social science? **NA.**
 - (g) Did you discuss the implications of your theoretical results for policy, practice, or further research in the social science domain? **NA.**
3. Additionally, if you are including theoretical proofs...
 - (a) Did you state the full set of assumptions of all theoretical results? **NA.**
 - (b) Did you include complete proofs of all theoretical results? **NA.**
4. Additionally, if you ran machine learning experiments...
 - (a) Did you include the code, data, and instructions needed to reproduce the main experimental results (either in the supplemental material or as a URL)? **NA.**
 - (b) Did you specify all the training details (e.g., data splits, hyperparameters, how they were chosen)? **NA.**
 - (c) Did you report error bars (e.g., with respect to the random seed after running experiments multiple times)? **NA.**
 - (d) Did you include the total amount of compute and the type of resources used (e.g., type of GPUs, internal cluster, or cloud provider)? **NA.**
 - (e) Do you justify how the proposed evaluation is sufficient and appropriate to the claims made? **NA.**
 - (f) Do you discuss what is "the cost" of misclassification and fault (in)tolerance? **NA.**
5. Additionally, if you are using existing assets (e.g., code, data, models) or curating/releasing new assets, **without compromising anonymity...**
 - (a) If your work uses existing assets, did you cite the creators? **NA.**
 - (b) Did you mention the license of the assets? **NA.**
 - (c) Did you include any new assets in the supplemental material or as a URL? **NA.**
 - (d) Did you discuss whether and how consent was obtained from people whose data you're using/curating? **NA.**
 - (e) Did you discuss whether the data you are using/curating contains personally identifiable information or offensive content? **NA.**

- (f) If you are curating or releasing new datasets, did you discuss how you intend to make your datasets FAIR? NA.
 - (g) If you are curating or releasing new datasets, did you create a Datasheet for the Dataset? NA.
6. Additionally, if you used crowdsourcing or conducted research with human subjects, **without compromising anonymity**...
- (a) Did you include the full text of instructions given to participants and screenshots? NA.
 - (b) Did you describe any potential participant risks, with mentions of Institutional Review Board (IRB) approvals? NA.
 - (c) Did you include the estimated hourly wage paid to participants and the total amount spent on participant compensation? NA.
 - (d) Did you discuss how data is stored, shared, and de-identified? NA.

Appendix A

Table 1: Availability of TikTok data for studying systemic risks in Romanian election interference incidents, classified by data category and access mechanism. Each row maps individual data points to their corresponding documentation sources and indicates their accessibility through the Research API and data donations.

Category	Data	Documentation	Research API	Data Donation
Content	Photo/ video	Privacy Policy	Yes	Yes
Content	Caption	Privacy Policy	Yes	Yes
Content	Create datetime	Privacy Policy	Yes	Yes
Content	Create location	Privacy Policy	No	Yes
Content	Hashtags	Privacy Policy	Yes	Yes
Content	User mentions	Privacy Policy	Yes	Yes
Content	Sound	Privacy Policy	Yes	Yes
Content	Transcription	Privacy Policy	Yes	No
Content	Language	Help Centre ¹¹	No	No
Content	Paid partnership tag	Branded Content Policy	No	Yes
Content	Detected content characteristics	Privacy Policy	No	No
Moderation	Reporting by users	Privacy Policy	No	No
Moderation	Moderation by platform	Privacy Policy	No	No
Account	Age	Privacy Policy	No	Limited
Account	Gender	Privacy Policy	No	No
Account	Language	Privacy Policy	Limited	Yes
Account	Bio	Privacy Policy	Yes	Yes
Account	Location	Privacy Policy	Yes	No
Account	Follower count	Privacy Policy	Yes	Yes
Account	Historical follower count	Privacy Policy	No	Yes
Account	Creation datetime	Privacy Policy	No	No
Account	Account type	Privacy Policy	No	No
Account	GPPPA status	Help Centre ¹²	No	No
Account	Verification status	Help Centre ¹³	Yes	No
Engagement	Like count	Privacy Policy	Yes	No
Engagement	Share count	Privacy Policy	Yes	No
Engagement	View count	Privacy Policy	Yes	No
Engagement	Favourite count	Privacy Policy	Yes	No
Engagement	Comment count	Privacy Policy	Yes	No
Engagement	Comment text	Privacy Policy	Limited	No
Engagement	Comment creation datetime	Privacy Policy	Limited	No
Engagement	Comment like count	Privacy Policy	Limited	No
Engagement	Comment reply count	Privacy Policy	Limited	No
Engagement	Historical engagement metrics	Privacy Policy	No	No
Engagement	Aggregate demographics	Privacy Policy	No	No
Network	Username of followers	Privacy Policy	Yes	Yes
Network	Username of following	Privacy Policy	Yes	Yes
Recommendation	FYP history	Privacy Policy	No	Limited
Recommendation	Algorithmic parameters	Help Centre ¹⁴	No	No
Recommendation	Aggregate demographics	Privacy Policy	No	No
Recommendation	Suggested search terms	Help Centre ¹⁵	No	No