Media and Communication
2025 • Volume 13 • Article 10733
https://doi.org/10.17645/mac.10733

ARTICLE

Open Access Journal

Behind the Screen: The Use of Facebook Accounts With Inauthentic Behavior During European Elections

Bogdan Oprea, Paula Pașnicu, Alexandru-Ninel Niculae, Constantin-Cozmin Bonciu, and Dragoș Tudorașcu-Dobre

Faculty of Journalism and Communication Sciences, University of Bucharest, Romania

Correspondence: Bogdan Oprea (bogdan.oprea@unibuc.ro)

Submitted: 19 May 2025 **Accepted:** 31 July 2025 **Published:** 4 September 2025

Issue: This article is part of the issue "Electoral Communication: European Elections in Times of (Poly)Crises" edited by Adriana Ștefănel (University of Bucharest) and Maria Romana Allegri (Sapienza University of Rome), fully open access at https://doi.org/10.17645/mac.i497

Abstract

Technology has reshaped political communication, allowing fake engagement to drive real influence in the democratic process. Hyperactive social media users, who are over-proportionally active in relation to the mean, are the new political activists, spreading partisan content at scale on social media platforms. Using The Authenticity Matrix tool, this study revealed Facebook accounts of hyperactive users exhibiting inauthentic behaviour that were used during the electoral campaign (May 10, 2024, to June 8, 2024) for the 2024 election of Romanian members of the European Parliament. The results indicate that, for some posts, up to 45% of shares were made by hyperactive users (four or more shares per post by the same account) and 33.9% by super-active users (10 or more times). This type of online behavior is considered by Meta as manipulation of "public opinion," "political discussion," and "public debate," and Meta's Community Standards is committed to preventing such behavior in the context of elections. Another key contribution of this research is the identification of dominant characteristics of hyperactive user accounts, using information publicly available on their social media profile, which provides insights into their specific features and helps users better identify them on social media. The article highlights that online social network platforms condemn these manipulative practices in theory, but they don't take sufficient measures to effectively reduce them in order to limit their impact on our societies.

Keywords

election campaign; Facebook; fake accounts; inauthentic behavior; manipulation; Meta; political communication; social media

1. Introduction

Online social networks (OSNs), like Facebook, Instagram, Twitter, and TikTok, have become part of our daily life, with 5.31 billion social media users around the world in April 2025, equating to 64.7% of the total global population (DataReportal, n.d.). They play a transformative role in modern society, fundamentally changing how people interact. Since social interaction has a crucial influence on shaping individual identity and building relationships between members of society, and the tradition of face-to-face communication and direct interaction in social contexts plays an important role in strengthening social ties, cultural exchange, and collective understanding, with the advent of social media, the way humans interact and communicate has undergone fundamental changes (Azzaakiyyah, 2023; Litt et al., 2020). OSNs are enabling users to connect with relatives and acquaintances, meet new people, share information, organize events, participate in social movements, directly access business opportunities worldwide, and build communities in a way humanity has never experienced before (Azzaakiyyah, 2023; Omar & Ondimu, 2024). Social media has democratized information and is shaping cultural trends and societal norms by promoting values and rights and by giving a voice to the previously unheard (Omar & Ondimu, 2024). By doing so, they have revolutionized public discourse, political communication, and campaign strategies (Omar & Ondimu, 2024; Rodenhäuser, 2023; Samoilenko, 2017). However, all these benefits are accompanied by challenges such as social isolation, unhealthy social comparisons, cultural appropriation, and the spread of disinformation (Azzaakiyyah, 2023; Gupta & Kaushal, 2017; Mughaid et al., 2023; Rodenhäuser, 2023; Voitovych et al., 2022). Since the widespread adoption of these platforms has also attracted malicious persons and entities that exploit them for fraudulent and misleading purposes, the rapid dissemination of both accurate information and disinformation, together with manipulated content, remains a central societal challenge. In this environment, 31% of EU citizens and 42% of Romanians tend to trust in OSNs, while 60% of EUs' citizens and 49% of Romanians tend not to trust OSNs (European Commission, 2024). At the same time, 68% of EUs' citizens and 79% of Romanians are declaring they have been exposed to disinformation and fake news over the past seven days (very often, often, sometimes; European Commission, 2023).

1.1. The Use of Fake Accounts in OSNs: Definitions and Taxonomy

On OSNs, disinformation and manipulation can find a tool with which audiences can be reached, potentially worldwide, but also micro-targeted, with an impact never-before-seen. On social media, manipulation actions aimed at determining a "social actor" (person, group, community) to think and act in a way compatible with the initiator's interests, and not with their own interests, have become common through the use of persuasion techniques at a rational and affective-emotional level, which intentionally distort the truth and inoculate a false perception of reality, leaving, however, the impression of freedom of thought and decision (Gherghel, 2009; Oprea, 2022). One of the ways in which manipulation on social media platforms is spread is by the creation and use of fake accounts. There is no consistent and widely accepted definition of fake accounts by industry and academia, which are also often referred to as "false accounts," "inauthentic accounts," "inauthentic behaviour accounts," "cyber troops," or "propagandists" (Bradshaw & Howard, 2017; Meta, n.d.-b, n.d.-c; Pamment et al., 2018; Weedon et al., 2017). Based on literature review, they are largely considered to be social media accounts designed to impersonate real users through fake personal information (names, photos) and/or behaviors (following, viewing, commenting, sharing), operated by humans, bots, or both, and which are created with the intent to mislead or deceive and to manipulate perceptions of popularity or influence (Huang & Liu, 2024; Moore, 2023; Oprea, 2022, 2023).

Scholars in social sciences and information technology propose several taxonomies for fake accounts or accounts with inauthentic behavior. A review of these classifications identifies several major types of accounts based on their operational characteristics and intent. A broad classification used in empirical research divides accounts into three main categories: real accounts, which are operated by genuine users with authentic identities; fake accounts that are typically controlled by humans that are hiding their identities and use false or misleading information, and the accounts are very often used for deceptive activities and to spread disinformation; and bot accounts, also known as social bots or Sybils, which are managed by automated software and can perform actions like posting, liking, or following at scale, often to manipulate engagement or disseminate content rapidly (Ferrara et al., 2016; Howard et al., 2018; Imperva, 2025; Michael, 2017; Tunç et al., 2024). One classification divides bots into two categories: good bots, such as search engine crawlers that index content; and bad bots that "are automated programs designed to perform harmful activities, such as scraping data, spamming, and launching denial-of-service attacks; these bots can mimic human behaviour, making them difficult to detect and block" (Imperva, 2025, p. 30). In 2024, automated traffic exceeded human-generated activity on the internet, constituting 51% of total web traffic (an increase from 49.6% in 2023 and 37.9% in 2018). Notably, bad bots accounted for 37% of all internet traffic, rising from 32% in 2023 and 20.4% in 2018 (Imperva, 2019, 2024, 2025).

Academics also refer to trolls. Moreau explains that "a troll is simply a user of an online social platform who deliberately tries to aggravate, annoy, disrupt, attack, offend or cause trouble by posting provocative and unconstructive content" (Moreau, 2017, as cited in Pamment et al., 2018, p. 62).

1.2. The Use of Fake Accounts in OSNs: Motivations and Threats

There are many motivations behind the creation and use of fake accounts. Since the OSNs allow individuals to construct social identities without any boundaries, these fake profiles can be used to conduct astroturfing campaigns, spam activities, spread malware, and phishing attacks, manipulate public opinion through information-psychological operations (infopsy), and violate user privacy, posing significant threats to individual users, the broader online ecosystem, and societies (Albayati & Altamimi, 2019a; Bailey & Samoilenko, 2017, as cited in Samoilenko, 2017; Gupta & Kaushal, 2017; Mughaid et al., 2023; Rodenhäuser, 2023; Voitovych et al., 2022). Pasieka et al. (2021, p. 259) consider that mass distribution of specially programmed false accounts is also used as a vehicle for legal cybercrime business, for organization of stuffing of information flows, mass theft of personal data, to affect social marketing, for creation of fake news feeds and fake votes, and even to create conditions for the deterioration of trust in social networks.

Researchers highlight that the use of social media fake accounts can have dangerous and far-reaching consequences on our societies and can pose serious threats. In a 2017 Facebook report (now unavailable), the platform referred to fake accounts as "false amplifiers" describing their role as "manipulating public opinion" and "manipulating political discussion" (Weedon et al., 2017, p. 5). Pamment et al. (2018) characterize the behavior of fake accounts as generating a "bandwagon" effect, noting that these users employ "imposter accounts" created to appear as though they are controlled by someone else and that they conduct so-called "false-flag operations." Bradshaw and Howard (2017, 2019) conceptualize these actors as organized cyber troops, sometimes consisting of "a handful of individuals managing hundreds of fake accounts" (Bradshaw & Howard, 2019, p. 17) and who "are government, military or political party teams committed to manipulating public opinion over social media" (Bradshaw & Howard, 2017, p. 3). Papakyriakopoulos et al. (2020) refer to such users as “hyperactive users” (HAUs) emphasizing their significant role in political discourse, emergence as opinion leaders, agenda-setting effect, and capacity to create an alternative image of public opinion, thereby strongly influencing Facebook’s recommendation systems (Papakyriakopoulos et al., 2020). In the meantime, the proliferation of fake accounts has even given rise to a black market for fake account services operated by both private companies and state agencies, further complicating efforts to maintain the integrity of social networks (Gupta & Kaushal, 2017; Hakimi et al., 2019).

1.3. The use of fake accounts on Facebook

1.3.1. Definitions and Taxonomy

Meta defines fake accounts as “accounts created with malicious intent to violate our policies and personal profiles created to represent a business, organization or non-human entity, such as a pet….Many of these accounts are used in spam campaigns and are financially motivated” (Meta, n.d.-b). The platform distinguishes between abusive fake accounts (created to cause harm) and user-misclassified accounts (such as those made for pets, which are not intended to deceive; Schultz, 2019). Meta considers the activity of fake accounts as “inauthentic behavior,” whose definition is periodically updated in Meta’s Community Standards since October 10, 2019. The current version, consulted on May 8, 2025, defines “inauthentic behavior” as “a variety of complex forms of deception, performed by a network of inauthentic assets controlled by the same individual or individuals, with the goal of deceiving Meta or our community or to evade enforcement under the Community Standards” (Meta, n.d.-c). This definition is placed in relation to the authenticity concept, which evokes a sense that something or someone is genuine (in the sense that it is what it says it is) and true (in the sense that it is factual; Johnston & Lane, 2019; Molleda, 2010). At the same time, the platform considers that fake accounts play a central role in what they call “coordinated inauthentic behavior,” defined as “coordinated efforts to manipulate public debate for a strategic goal” which “is often associated with civic or political content” (Meta, n.d.-c). Also, the platform is referring to “inauthentic meta assets” which consist of accounts, pages, groups, and other (Meta, n.d.-c). In a 2017 Facebook report, which is currently no longer available, the platform considered that the fake accounts “have an ideological rather than a financial motivation,” and, that in some instances, they “attempt to influence political opinions on social media with large numbers of sparsely populated fake accounts that are used to share and engage with content at high volumes,” but, “in other cases, the networks may involve behavior by a smaller number of carefully curated accounts that exhibit authentic characteristics with well-developed online personas,” “coordinated people who are dedicated to operating inauthentic accounts,” their activity “can include topics around political figures or parties, divisive policies, religion, national governments, nations and/or ethnicities, institutions, or current events” (Weedon et al., 2017, p. 9).

Considering Meta’s Community Standards terminology, for research on the sharing type of engagement, Oprea identifies four categories of users in terms of Facebook posts sharing behavior:

- Normal user (NU): the account whose user has shared a specific post only once, either on their own timeline or in a group;
- Moderately active user (MAU): the account whose user has shared the same post twice or three times, either on their own timeline or on their own timeline and into one or more groups, or only into one or more groups;

- Hyperactive user (HAU): the account whose user has shared the same post four or more times, either on their own timeline or on their own timeline and into one or more groups, or only into one or more groups;
- Super-active user (SAU): the account whose user has shared the same post ten or more times, either on their own timeline or on their own timeline and into one or more groups, or only into one or more groups. (Oprea, 2023, p. 62).

While Meta defines inauthentic behavior as activity carried out by networks of inauthentic assets controlled by the same individual or individuals with the intention to deceive, it is important to note that not all inauthentic behavior originates from inauthentic accounts. A HAU or SAU displays inauthentic behavior, but it is not necessarily a fake account or one operated with malicious intent; it could simply be a hyperactive supporter or activist who is over-proportionally active in relation to the mean and his actions could simply reflect legitimate forms of democratic participation.

1.3.2. Preventing Measures

In the Community Standards, Meta (n.d.-c) explicitly states that the platform has a commitment to authenticity:

> In line with our commitment to authenticity, we don't allow people to misrepresent themselves on our services, use fake accounts, artificially boost the popularity of content, or engage in behaviors designed to enable other violations under our Community Standards. Inauthentic behavior refers to a variety of complex forms of deception, performed by a network of inauthentic assets controlled by the same individual or individuals, with the goal of deceiving Meta or our community or to evade enforcement under the Community Standards.

Meta (n.d.-c) also states that they:

> Are committed to preventing inauthentic behavior in the context of elections—these enforcement actions and standards apply agnostic of content, political or otherwise. This policy is intended to protect the authenticity of debate and discussion on our services, and create a space where people can trust the people and communities they interact with.

In this respect, Meta refers to three type of "inauthentic meta assets" that are not allowed on the platform:

> To deceive Meta or our users about the identity, purpose, or origin of an audience or the entity that they represent, or the popularity of content or assets on our services, or a Meta asset's ownership or control network…to evade enforcement under the Community Standards [and the] misuse Meta reporting systems to harass, intimidate or silence others. (Meta, n.d.-c)

The platform also mentions five types of complex deception through the use of Meta assets which they don't allow engaging with: "inauthentic distribution," "using a connected network of inauthentic Meta assets to increase the distribution of content, in order to mislead Meta or its users about the popularity of the content in question"); "inauthentic audience building," "using inauthentic Meta assets to increase the viewership or following of network assets, in order to mislead Meta or its users about the origin, ownership or purpose of an asset or assets"; "foreign inauthentic behavior," "foreign entities using inauthentic Meta assets to falsely represent a domestic or local voice, in order to deceive an audience about the identity, purpose or origin of the entity they represent"; "inauthentic engagement," "using a connected network of inauthentic Meta assets to deliver substantial quantities of fake engagement in ways designed to look authentic, in order to deceive Meta and its users about the popularity of content"; and "substantially similar deceptions," "other substantially similar claimed or actual efforts by relatively sophisticated, connected networks of inauthentic Meta assets to deceive Meta or its users about the origin, popularity, or purpose of content" (Meta, n.d.-c).

Despite these policies, the occurrence of fake accounts on Facebook remains at impressive proportions. With 3.07 billion users in January 2025, Meta officially reported that, between October 2017 and December 2024, it managed to identify and delete from Facebook 35.58 billion fake accounts, which is equivalent to almost 12 times the number of users of the platform and over 4.4 times the global population (DataReportal, n.d.; Meta, n.d.-b; World Bank Group, 2025).

2. Fake Accounts Detection Approaches

2.1. General Overview

With the increasing prevalence of fake accounts on social media, researchers from interdisciplinary fields have looked for ways to detect them as part of either OSNs: self-regulatory strategies—Meta's Community Standards (Meta, n.d.-a), X rules and policies (X, 2025); co-regulations—EU's 2018 Code of Practice on Disinformation, strengthened in 2022 (European Commission, 2022); or even legislation—EU's 2022 Digital Services Act (European Parliament and the Council Regulation of 19 October 2022, 2022), Australia's Sharing of Abhorrent Violent Material 2019 Bill (Parliament of Australia, 2019), and Germany's 2017 Netzwerkdurchsetzungsgesetz (Network Enforcement Act; Bundesministerium der Justiz, 2017). By analyzing the literature, we can consider four major approaches to OSNs fake news detection:

- Feature-based detection: Analysis of individual account characteristics such as user behavior, activity patterns, profile completeness (Khaled et al., 2018; Oprea, 2024; Romanov et al., 2017);
- Graph-based and coordinated activity detection: Methods that identify groups of accounts acting in concert and in other abnormal patterns (Boshmaf et al., 2016; Graham et al., 2024; Gruzd et al., 2022; Padmavathi & Vaisshnavi, 2024);
- Machine learning techniques: Overview of algorithms used (e.g., support vector machines, neural networks, decision trees), their performance, and the features they leverage (Aljabri et al., 2023; Arega et al., 2023; Jadhav et al., 2021; Khaled et al., 2018; Mughaid et al., 2023);
- Hybrid and emerging methods: Discussion of combined approaches and the use of advanced analytics, such as natural language processing, and web scraping for content analysis (Abualigah et al., 2021; Arega et al., 2023).

The proposed fake account identification models have different success rates, which can achieve quite high levels of performance using computational models and algorithms, as 93% (Arega et al., 2023) or 97.1% (Mughaid et al., 2023) for support vector machine, and even 98.25% for K-Nearest Neighbor, 99.1% for artificial neural network (Azami & Passi, 2024), and 99.29, for decision tree algorithm (Elyusufi et al., 2019). Testing these models across a diverse research corpus remains a significant challenge. However, such evaluation is essential for developing models with robust and generalizable accuracy, thereby enabling their widespread adoption. Advancements in this area have the potential to substantially reduce the prevalence of fake accounts on social media platforms.

2.2. *"The Authenticity Matrix" Tool*

Facebook, like all major OSNs, has increasingly restrictive API (application programming interface) protocol policies that don't allow for automated data collection, including by researchers (Gotfredsen & Dowling, 2024; Hothman, 2019; Walker et al., 2019). In constant change of policies and with increasingly limited access to data, currently, researchers and journalists can access the content archive from Facebook through Meta Content Library and Content Library API, but only "posts to pages, groups, events and public profiles belonging to widely-known individuals and organizations" (Meta, 2025). Therefore, automated tools can only use data to which Meta offers access, but, in order to identify fake accounts and accounts with inauthentic behavior, data relating to accounts that don't belong to "widely-known individuals and organizations" are impossible to be collected. This leaves room for those who use such fake account manipulation techniques to create and widely use accounts that do not fall into these categories, of no widely-known individuals and organizations, and which thus cannot be accessed by researchers and journalists.

Oprea's Authenticity Matrix tool to detect accounts with inauthentic behavior was developed to address this issue and to provide scientific data about the real extent of the use of accounts with inauthentic behavior (Oprea, 2024). Using a Likert scale model, this tool analyzes all public information that can be manually accessed on Facebook accounts by any account that is not restricted and proposes an analysis matrix that allows establishing a degree of probability that a specific Facebook account has inauthentic behavior. The Authenticity Matrix is a methodological tool designed to assess the authenticity of Facebook's accounts by analyzing three core dimensions: general/personal account information, account activity, and likes/interactions. Using a metric scale from 0 to 100 points, this matrix quantifies authenticity levels, enabling researchers to systematically evaluate account authenticity by placing them in one of three categories: accounts with authentic behavior, accounts with an average probability of inauthentic behavior, or, respectively, accounts with inauthentic behavior (Oprea, 2024).

The Authenticity Matrix uses a feature-based detection approach (see Section 2.1) and conducts a multi-dimensional assessment of the account's authenticity based on several indicators. Two classes of indicators, account activity and likes/interactions, express the level of engagement, while general/personal account information indicators express a degree of transparency, which is required by Meta's Community Standards. A user may display intense, atypical engagement while still retaining an overall profile configuration that does not meet Meta's policies, so this tool cumulatively analyzes these indicators. The reliability of the Authenticity Matrix stems from its comprehensive design, which considers multiple indicators of authenticity rather than focusing exclusively on activity behavior (see Section 2.1).

It is essential to highlight that tools using machine learning models applied on the same type of indicators as the Authenticity Matrix (e.g., account names, profile photos, account activity, etc.) were previously developed (see Albayati & Altamimi, 2019b). Presently, they cannot be used on the corpus of this research due to Meta's restrictive API policies, especially since 2019 (Gotfredsen & Dowling, 2024; Hothman, 2019; Walker et al., 2019). In this respect, the Authenticity Matrix manual approach finds its relevance since it can be used despite any restrictions on automated tools.

3. Manipulation and Democratic Processes

Advancements in communication technology over the last decades have enabled mass communication on an unprecedented scale. These technologies now facilitate direct and unmediated interactions between actors of influence (public institutions, private organizations, politicians, political parties, etc.) and their audiences while, simultaneously, providing the capacity to reach global populations. Technologies such as OSNs have been widely adopted and have become communication tools, including for political communication. Electoral campaigns are one of the key moments of public debate and a top opportunity for political actors to communicate and provide citizens with the necessary information to make voting decisions (Casero-Ripollés et al., 2025). In recent years, the spread of manipulation and disinformation has intensified before, during, and after these periods, altering the democratic process of voting (Bradshaw et al., 2020; Casero-Ripollés et al., 2025; European External Action Service, 2024).

The election month is the moment when the manipulation activity increases:

> With threat actors adopting a more varied modus operandi and seizing heightened collective attention towards the topic of elections….In this phase, the networks created can be activated to launch attacks aimed at undermining the reputation of candidates and political parties. (European External Action Service, 2024)

The 2024 European Parliament Elections were among the electoral events with the most manipulation incidents recorded by the European External Action Service (2025), the foreign affairs service of the EU. Also, the European Digital Media Observatory Task Force on the 2024 European Parliament Elections reported that, in the last months before the elections, EU-related disinformation increased from 5% in January to 15% in May, the highest level since their monitoring began (European Digital Media Observatory Task Force, 2024). In a recent analysis of the electoral disinformation during the 2024 European Parliament Elections, Casero-Ripollés et al. (2025) identified that Southern Europe (41.7%) and Eastern Europe (31.4%) accumulated the highest percentage of electoral disinformation, with Romania considered to be a South-Eastern country, and with Facebook being the second origin source of false information (21.9%) after X (32.4%) and before legacy media (13.3%; Casero-Ripollés et al., 2025).

Since the previous European Parliament Elections in 2019 followed Brexit and the US 2016 election, when large manipulation campaigns were reported (Lilkov, 2019), concerns about manipulation and disinformation were raised by media outlets, NGOs, and EU institutions and officials (Avaaz, 2019; Scott, 2019). At the EU level, unprecedented cooperation took place in recent years to support the resilience of the member states. The European Commission, EUs executive branch, started a coordinated action on manipulation and disinformation mitigation by launching: a strategic communication task force to address this issue in 2015 (European External Action Service East StratCom Task Force); a co-regulatory code with OSNs platforms in 2018 (The Code of Practice Against Disinformation); a rapid alert system at EU institutions and member states levels in 2019; and a hub for independent community working to combat disinformation in 2020 (European Digital Media Observatory). It also created several regulatory measures: The Digital Services Act in 2020; the European Media Freedom Act in 2024; and the regulation of the transparency and targeting of political advertising in 2024 (European Commission, n.d.; European Commission, 2025; Navarro et al., 2025). Also, at the national level in Romania, local initiatives have been implemented to combat manipulation and disinformation, ranging from media literacy programs run by NGOs and an optional subject on the same topic implemented in public schools, to other broader institutional measures (Ministry of Education, 2022; "Programul de Educație Media," 2025).

Romania's information ecosystem exhibits multiple vulnerabilities such as unclear media ownership and funding, distrust in traditional media, the use of social media for news, large exposure to anti-EU and anti-Western narratives, and a general social context which has lately been characterized by political instability (Durach et al., 2025; Institutul Român pentru Evaluare și Strategie, 2024; Radu, 2025; Toma & Suciu, 2024). At the same time, trust in politicians and political parties in Romania is the lowest among institutions, with 86% of the population saying they have little, very little, and no trust in political parties and 90% stating the same for politicians (Centrul de Sociologie Urbană și Regională, 2024; Institutul Român pentru Evaluare și Strategie, 2024).

In this general climate marked, on the one hand, by profund distrust, external interference, and multiple vulnerabilities of the Romania's information ecosystem, and, on the other hand, by measures from European institutions, local civil society, and authorities to combat manipulation and disinformation, this study aims to understand if top political parties are complaiying with these efforts. In this respect, the study aims to assess whether political parties and electoral alliances taking part in the 2024 election of Romanian members of the European Parliament were engaging in manipulation strategies on social media despite the increasing number of institutional and civic countermeasures.

4. Research Questions and Objectives

This study aims to determine whether accounts exhibiting inauthentic behavior were employed during the 2024 Romanian European Parliament election campaigns on OSNs. Such manipulation would involve inauthentic influence of Facebook recommendation algorithms (through shares made by accounts specially created for this purpose), thereby increasing the visibility of political content beyond what would have occurred through organic engagement alone. Furthermore, the research investigates whether accounts with inauthentic behavior used to promote specific political parties or electoral alliances disclosed their political affiliations or the potential nature of their involvement or support.

To this end, the following research questions have been formulated:

> RQ1: To what extent were social media accounts displaying inauthentic behavior utilized during the 2024 election of Romanian members of the European Parliament campaign and what is the scale of their use?
>
> RQ2: How were accounts with inauthentic behavior deployed throughout the campaign?
>
> RQ3: What are the characteristics of social media accounts with inauthentic behavior?

To address the above RQs, this study analyzed the most shared posts in the election campaign on the official Facebook pages of the top four political parties or electoral alliances taking part in the 2024 election of Romanian members of the European Parliament in terms of the number of votes obtained (European

Parliament, 2024). We chose shares as the type of engagement because they are an important measurement for online engagement, they measure the explicit actions of a user with the content, people are more likely to trust information that is shared by friends and family, and because a post is more popular as it gets more shares, which also increases its visibility on the platform (Corzo, 2021; Moro et al., 2016, as cited in Corbu et al., 2022; Oprea, 2023). More visibility means including a post in as many users' news feeds as possible, which, in this case, means exposing more citizens to a specific political message. To do so, politicians, their teams, or their supporters could use a number of social media fake accounts or accounts with inauthentic behavior specifically created for this purpose, and this would mean, according to Facebook, a violation of Community Standards but also a form of manipulation of public opinion and political discussion and a practice of misleading people (Meta, n.d.-c; Weedon et al., 2017).

5. Methodology

5.1. Dataset

This preliminary explanatory research analyzed the three most shared posts in the election campaign on the official Facebook pages of the top four political parties or electoral alliances taking part in the 2024 election of Romanian members of the European Parliament in terms of the number of votes obtained, according to the results of the elections. We analysed all posts' content that was published between May 10, 2024, 00 AM, and June 8, 2024, 7 AM, on the pages of Partidul Social Democrat (PSD; from the Alianța PSD–PNL), Partidul Național Liberal (PNL; from Alianța PSD–PNL), Alianța pentru Unirea Românilor (AUR), and Uniunea Salvați România (USR; from the Alianța Dreapta Unită; Autoritatea Electorală Permanentă, 2019; European Parliament, 2024). During this period, the PSD page had 154 posts, the PNL page had 174 posts, the AUR page had 67 posts, and the USR page had 175 posts.

Data was collected manually, between December 2024–May 2025, using four personal regular Facebook accounts of the team. The manual collection process was the only one available because, due to Facebook's API restrictive policies, it is the only way to access the data, shares, and the Facebook accounts and groups in which they were distributed, which were needed for this research. The data was gathered on Microsoft Word documents and tabular spreadsheets in Microsoft Excel for which the search function was applied for the names of the accounts that shared the posts in order to identify accounts that made multiple shares and to monitor the number of shares for each account. Because of the large amount of data and the lack of an electronic data collection tool, we chose the top three most shared posts on each Facebook page during the election campaign period. The research corpus thus covered 6.7% of all shares during the analyzed period, up to a total of 70,293 shares. The posts included in the corpus have 4,476 shares where we could view the account of the user who shared them and the place where they were shared (on their own timeline, on their own timeline and in one or more groups, or only in several groups). Due to the privacy settings of Facebook, not all the shared data could be accessed using personal regular Facebook accounts, with the platform displaying at the end of the accessible shares the "some posts may not appear here due to their privacy settings" message. At the same time, in the case of AUR's page, even using high-end PCs, the Facebook platform stopped loading and would eventually crash into a blank screen. For this reason, for PSD's page, we could collect data for 8.7% of shares, 8.9% for PNL, 6.3% for AUR, and 6.9% for USR (Table 1).

Table 1. Research corpus vs research field (absolute number and percentage).

Page name	Total shares per period	Total shares of the analyzed posts	Total shares analyzed
PSD	4,723	825 17.5%	409 8.7%
PNL	4,063	823 20.3%	360 8.9%
AUR	48,150	11,514 26.3%	3,027 6.3%
USR	13,357	1,749 13.1%	924 6.9%

Taking into consideration that for such types of accounts, due to Facebook's restrictive policies, only manual collection is possible, this corpus provides sufficient data to identify inauthentic behavior in the share activity on these political pages.

Given the nature and size of the dataset, as well as the exploratory aim of the study, we opted for a qualitative-comparative approach supported by descriptive statistics. The relatively small and heterogeneous sample of accounts, combined with the non-randomized nature of data collection, led us to an analytical depth and transparency approach through structured coding and detailed qualitative documentation, which better serves the purpose of capturing patterns of inauthentic behavior and rhetorical strategies in the sample studied.

5.2. Findings

5.2.1. Engagement of Accounts With Inauthentic Behavior

This study identified Facebook accounts displaying inauthentic behavior that were actively engaged in the 2024 election campaign of Romanian members of the European Parliament on the official pages of the four political parties or electoral alliances. To address RQ1 and RQ2, the analysis focused on the relationship between the number of shares and the accounts responsible for sharing, particularly examining instances where individual accounts shared the same post at least four times, being a HAU.

Compared to typical posts outside the campaign period, one month before and after (April 10–May 9, 2024, and June 10–July 9, 2024), the analyzed posts proved a higher popularity, as measured by the number of shares. Notably, 23.2% of all shares were hyperactive shares made by HAUs (defined as users who shared the same post four or more times, either on their own timeline or on their own timeline and into one or more groups, or only into one or more groups). In some cases, hyperactive shares accounted for up to 45% of the total shares of the same post. These findings indicate a significant user engagement in repeatedly sharing posts from official political parties or electoral alliances' pages. Across pages, the proportion of HAU shares ranged from 14.2% to 45% (USR), 20.6% to 28.1% (AUR), 0% to 26.2% (PNL), and 0% to 17.1% (PSD) (Table 2). These results underscore a significant level of HAU involvement in sharing activities. The analysis also revealed the presence of highly prolific users, including accounts that shared the same post 31 and 22 times, patterns of engagement that are indicative of inauthentic behavior.

Table 2. Distribution of HAUs and SAUs from total shares.

Page name	Post no.	Percentage of HAUs from total shares	Percentage of SAUs from total shares
PSD	PSD1	17.1	12
	PSD2	6.4	6.4
	PSD3	0	0
PNL	PNL1	26.2	10.3
	PNL2	6.6	0
	PNL3	0	0
AUR	AUR1	28.1	16.3
	AUR2	22	8.1
	AUR3	20.6	6.1
USR	USR1	14.2	3.9
	USR2	45	33.9
	USR2	18.6	8

The data demonstrate that inauthentic behavior accounts were used to amplify candidate posts through repeated sharing (RQ1), with even 33.9% of shares made by users sharing the same post 10 or more times (RQ2).

5.2.2. Profile of Accounts With Inauthentic Behavior

To address RQ3, the study analyzed publicly available information from HAU accounts. Several characteristics emerged (Table 3). Firstly, 7.1% of HAUs used account names that did not conform to typical human naming conventions in accordance with Meta's Community Standards, and 18.8% lacked a profile picture, a cover photo depicting a human, or displayed other signs of inauthenticity.

In regards to HAUs posting regularity, we found that: 61.6% of HAUs posted more than four times per day or didn't post at all for at least 30 consecutive days; 45.5% posted 10 or more times per day; also, some users posted on their account's timeline 187 posts/day (taking into account the time between the first and the last one, an average of one post every seven minutes and 22 seconds), 184 posts/day (an average of one post every four minutes, approximately), 179 posts/day (an average of one post every one minute and 48 seconds), 166 posts/day (an average of one post every 4 minutes, approximately), 158 posts/day (an average of one post every 20 seconds), 145 posts/day (an average of one post every five minutes, approximately), or 139 posts/day (an average of one post every one minute and 45 seconds). There were accounts that posted as many as 75 posts in 10 minutes, once every eight seconds.

Only 16.1% of HAUs had no "likes" in any of the profile categories, and 40.2% of HAUs only posted on their account posts on political, civic, or other topics currently on the public agenda, and not personal posts, which would indicate authenticity. Some HAUs don't have any friends or less than 10 friends on their accounts (17%), and 18.8% of HAUs don't have any personal photos or videos on their accounts.

Only 4.5% of HAUs disclosed political affiliation on their "about" profile section, meaning 95.5% did not, despite repeated sharing of political content; however, 27.7% displayed political support through profile pictures, cover photos, or profile picture frames.

Table 3. Profile of accounts with inauthentic behavior.

Characteristics of HAUs profile	Percentage from the total of HAUs
Don't disclose political affiliation on their "About" profile section	95.5%
Post more than four times per day or don't post at all for at least 30 consecutive days	61.6%
Post 10 or more times per day	45.5%
Post on their account only posts on political, civic, or other topics currently on the public agenda, and not personal posts	40.2%
Display political support through profile pictures, cover photos, or profile picture frames	27.7%
Don't have any personal photos or videos on their accounts	18.8%
Lack a profile picture, a cover photo depicting a human, or displayed other signs of inauthenticity	18.8%
Don't have any or fewer than 10 friends on their accounts	17%
No "likes" in any of the profile categories	16.1%
Use account names that do not conform to typical human naming conventions in accordance with Meta's Community Standards	7.1%

After applying Oprea's (2024) Authenticity Matrix tool, we have identified that from the hyperactive accounts, 38.4% are accounts with authentic behavior, 42.9% are accounts with an average probability of inauthentic behavior, and 18.8% are accounts with inauthentic behavior (Figure 1).

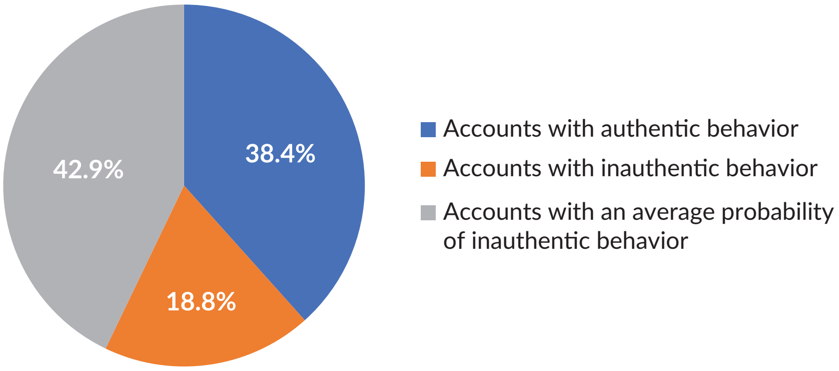

Figure 1. Authenticity behavior range of profile of accounts.

These findings highlight dominant traits of accounts displaying inauthentic behavior on OSN platforms (RQ3), such as the prevalence of human/non-human username and profile picture, the type of activity on the account's timeline, the level of transparency in terms of affiliation and support for a political party or electoral alliance, and the level of involvement in the multiple distribution activities of the analyzed posts. Some accounts were inactive for weeks or months before suddenly becoming highly active, often posting dozens of times per day, predominantly with political or civic content.

5.3. Discussions

The proliferation of digital manipulation is recognized as a significant threat to democratic processes. This study contributes by demonstrating that Facebook accounts can be used inauthentically to amplify political messages during the 2024 election campaign of Romanian members of the European Parliament. Facebook itself classifies such activity as "manipulating public opinion," "manipulating political discussion," and "manipulat[ing] public debate" (Meta, n.d.-c; Weedon et al., 2017), targeting the platform's recommendation algorithms through HAU behavior.

A key contribution of this research is the identification of dominant characteristics of HAU accounts, using information publicly available on their social media profile. This provides insights into their specific features and may help users to better identify them on social media. These findings need to be put in the broader context of algorithms that shape the digital world, in which we, as human beings, are spending more and more of our time—six hours and 38 minutes, on average, at the global level for 2024 (we are social & Meltwater, 2025). The question is how considerable is "the social power of algorithms" (Beer, 2020) since, as some scholars suggest, algorithms "construct regimes of power and knowledge" (Kushner, 2013) and we live under an "algorithmic governance" (Katzenbach & Ulbricht, 2019). These findings must be contextualized within the broader influence of algorithms on digital life as algorithms increasingly shape information exposure and public discourse.

Our research extends existing literature by showing that inauthentic behavior is also prevalent on political party pages and top political leaders and that such behavior includes the strategic use of the share engagement functionality (Oprea, 2023; Papakyriakopoulos et al., 2020). Shares increase post visibility and can serve as signals of newsworthiness for traditional media (Zhang et al., 2018). Therefore, increasing the number of shares of political posts is essential for broadening public exposure to these messages, particularly during election campaigns when political stakes are heightened. This study does not seek to determine whether such sharing activity is intentional or unintentional, nor does it aim to establish whether the accounts involved were specifically created for this purpose. Previous research has documented instances of coordinated inauthentic behavior in the sharing of political content (Giglietto et al., 2020; Graham et al., 2024; Gruzd et al., 2022) and it is empirically recognized that political digital marketing specialists may employ false amplifiers, coordinated individuals managing inauthentic accounts, to boost social media content (Weedon et al., 2017). Meanwhile, the present study does not attempt to identify the authenticity of the accounts analyzed, but their behavior. Consequently, it may include false amplifiers, fake accounts operated by bots or trolls, or genuine accounts of ordinary users who, motivated by personal political conviction, actively share posts from their preferred political parties (Giglietto et al., 2020; Weedon et al., 2017). Nevertheless, the empirically observed behaviors violate Meta's Community Standards.

Regarding the impact, our study found that, for the corpus we analyzed, 23.2% of shares were made by HAUs (four or more shares per post by the same account). In the meantime, for some posts, the hyperactive shares accounted for up to 45% of the share's total. The shares of some posts made by SAUs were 33.9%

(posted 10 or more times). Taking into consideration the limitations of the tool we used, the results of the study still align with prior research, such as Papakyriakopoulos et al. (2020) who found HAUs accounted for about 25.8% of comments and 26.4% of likes on German political party Facebook pages, and Oprea (2023) who found that 18.3% of shares were made by HAU's (four or more times) and 46.3%, by SAU's (10 or more times). This practice appears intended to manipulate Facebook's recommendation algorithms, increasing the exposure of political content beyond what would occur organically. This type of behavior has two direct consequences: (a) it increases user exposure to a specific political message beyond what would occur if the content's popularity evolved organically within the platform, and (b) such amplification can further elevate the message's public visibility by prompting coverage in traditional media outlets, which may use indicators of high engagement or discussion on social media as criteria for determining newsworthiness.

An interesting finding is that, among HAUs, 38.4% were considered authentic by the analysis tool. This suggests that legitimate political engagement or activism can produce high-activity patterns that mimic inauthentic behavior and, furthermore, justifies the need for a multi-indicator approach to authenticity detection. This type of authentic behavior is healthy for political debate, being the very basis of the democratic processes. However, these authentic grassroots voices are often overshadowed by accounts operated with the purpose of distorting public discourse. Our focus as a society must be towards bringing them back to the center of the public debate and also to do the necessary efforts to clean the information ecosystem of disturbing actors and activities.

The research also developed a general profile of HAUs: 7.1% of them didn't use human names; 18.8% didn't have profile images featuring human faces; 17% didn't have any friends or fewer than 10 friends on their accounts; and 18.8% didn't have any personal photos or videos on their timeline. Also, 16.1% of HAUs had no "likes" in any of the profile categories. HAUs that posted more than four times per day or didn't post at all for at least 30 consecutive days were 61.6%, and 40.2% only posted on their account posts on political, civic, or other topics currently on the public agenda, with no personal posts. Although they are obviously involved in sharing political content on the platform, 95.5% of HAUs did not disclose political affiliation on their profile, but 27.7% displayed their political support through profile pictures, cover photos, or profile picture frames.

These findings are relevant in three ways. On the one hand, it allows a better understanding of the specifics of these accounts and helps to shape a profile for the inauthentic behavior accounts based on the prevalence of human/non-human user name and profile picture, the type of activity on the account's timeline, the level of transparency in terms of affiliation and support for a political party or candidate, and the level of involvement in the multiple sharing activities of the analyzed posts. On the other hand, it makes this type of account easier to recognize by scholars, fact-checking journalists, and the general public. At the same time, the findings highlight the extensive use of inauthentic accounts on official political parties' pages during sensitive periods, such as election campaigns. Given the reported deletion of 35.58 billion fake accounts by Meta in recent years (Meta, n.d.-b), social media platforms should collaborate more closely with researchers to address manipulation and disinformation. Enhanced data access for researchers and journalists, such as relaxed API protocol restrictions, would facilitate the development of tools for identifying inauthentic accounts on OSNs. This would be in line with Meta Community Standards' commitments to authenticity and to the prevention of inauthentic behavior, which states that the platform doesn't allow people to misrepresent themselves, to use fake accounts, or to artificially boost the popularity of content (Meta, n.d.-c). Also, this study employed a data manual collection approach to identify inauthentic accounts on Facebook.

While automated machine-learning models exist and can achieve high performances (e.g., Arega et al., 2023; Azami & Passi, 2024; Elyusufi et al., 2019; Mughaid et al., 2023), they are limited by Facebook's restrictive API protocol policies which limit access to information. Relevant data, such as where a post was shared (on an account/page or on a group), are only accessible through manual searches, and this type of information can be relevant to understand the coordination character of some accounts, like the behavior and characteristics of HAUs' accounts. Here is where current research brings another relevant contribution.

The research has several important limitations, especially because of the manual data collection process. First, only a subset of posts from each candidate's page was included (6.7% of all shares during the analyzed period). Another limitation is the potential level of inaccuracy for the data collected due to human error, which we tried to limit by cross-checking the collected data. We also faced constraints to data access because of: the use of personal Facebook accounts; the dynamic nature of social media where posts, accounts, and interactions, can be deleted, blocked, etc.; and of temporal validity for data, since data was collected months after the election campaign and posts and account content could have been altered. At the same time, this tool may overlook users whose activity patterns are inauthentic, yet who are genuine supporters or activists. As such, methods focused on detecting coordinated behavior or hyperactivity—as proposed by Graham et al. (2024), Gruzd et al. (2022), or Giglietto et al. (2020)—could complement our approach by identifying accounts that may be strategically curated to appear authentic, yet act in ways consistent with manipulation or astroturfing. At the same time, data interpretation using a manual tool may have a degree of subjectivity, potentially influencing the final outcomes; to mitigate this limitation, we cross-checked the results to enhance the accuracy of the analysis. All these limits pose challenges for the reliability of this research and, in general, for research conducted on Facebook and other OSNs. Overall, they underscore the need for improved data access and transparency from social media platforms to enable more comprehensive and accurate research on inauthentic behavior and its implications for democratic processes.

6. Conclusions

This study is a preliminary investigation on Facebook that demonstrates the use of accounts to amplify the visibility of political messages posted on the official pages of the top four political parties or electoral alliances taking part in the 2024 election campaign of Romanian members of the European Parliament. The analysis reveals the use of accounts engaged in behaviors classified as inauthentic according to Meta's Community Standards (Meta, n.d.-c), specifically aiming to misrepresent the popularity of certain content; such inauthentic activity primarily involved the repeated sharing of posts, either on their own timelines or across multiple groups. Facebook itself classifies such activity as "manipulating public opinion," "manipulating political discussion," and "manipulat[ing] public debate," and commits to preventing this type of behavior on the platform (Meta, n.d.-c; Weedon et al., 2017).

Data shows that political actors, their communication teams, and/or their supporters use—or at least tolerate the use of—manipulative techniques in political debate, despite the public perception of the scale of manipulation and disinformation and the negative consequences these practices have on the democratic process and on our societies. With posts where nearly half of the shares (45%) were made by HAUs, and the share engagement being one of the two main types of measurements for online engagement, this practice could raise concerns about the integrity of public discourse and the democratic process. Also, these findings concern political parties and electoral alliances comprising the leading political forces in an EU and NATO member state, Romania, and to an electoral process at the European level, thus, a vote that is neither local nor isolated; despite all these, the manipulation of public discourse is not only tolerated, but increasingly prevalent. Furthermore, the scale of disinformation on Facebook has long been the subject of public debate in Europe and in Romania. OSNs, such as TikTok and Instagram, which have surged in popularity, operate with different user interaction models (for instance, they do not display who has shared a post), enabling alternative forms of manipulation that remain largely non-transparent and unknown, not only to the public but also to the research community. If such extensive manipulation is already normalized on a platform as heavily exposed to manipulation and disinformation as Facebook, it is plausible that on newly adopted OSNs, which are less transparent, these practices may be even more effectively concealed, carrying potentially greater and more damaging consequences for democratic societies.

These results consider the practical implications and show that, even if the OSN platforms condemn such practices in theory, they are not taking the necessary measures to effectively limit them. Thus, the relevance of these findings is significant for five main reasons. First, it provides OSN platforms and legislators with an understanding that additional measures (procedural–legislative, co-regulatory, and self-regulatory, but also of a technical nature) are needed to reduce these manipulation practices. Also, the research identified several predominant characteristics of these accounts with inauthentic behavior, offering valuable insights into their operationalization and providing potential markers for their identification. These findings have practical implications for enhancing fact-checking methodologies, benefitting both professional fact-checkers and everyday social media users. Furthermore, this article aims to raise awareness among the general audience—and, especially, for the actors involved in operating accounts with inauthentic behavior on a large scale—of the impact this practice has, the fact that it is a manipulative activity (in Meta's own words), and that it violates the Meta's Community Standards and, more importantly, basic deontological principles. This article underscores the necessity for more sophisticated technical solutions to detect fake accounts and accounts with inauthentic behavior that contravene OSN's community standards and terms and conditions rules. Additionally, policy interventions such as limiting the number of times a single account can share the same post may help mitigate the spread of inauthentic content. Finally, this research advocates for: a multi-solution approach to manipulation on OSN's, clear disclosure on how algorithms influence content visibility, a larger access to data for researchers and journalists, and a stronger enforcement policy to address this issue by empowering trust and safety specialists and content moderators worldwide with necessary resources.

Since, because of the limitations, this study is just a preliminary investigation, similar research should be carried out on corpora from other countries and across different OSNs, using diverse analytical methods, in order to better understand the true scale and societal impact of accounts with inauthentic behaviour operating within the vast ecosystem of billions of user profiles. They should be the ground for more robust legislative and co-regulatory measures. Also, they should argue for support from the media and civil society which is essential in contributing to the broader efforts of monitoring these practices and educating the public. Finally, greater awareness is needed among political actors, their communication teams, and even political supporters or activists, regarding the destructive impact such practices have on democratic processes and on our societies.

Funding

Publication of this article in open access was made possible through the institutional membership agreement between the University of Bucharest–Faculty of Journalism and Communication Studies and Cogitatio Press.

Conflict of Interests

The co-author Cosmin Bonciu is a member of the Social Democratic Party (Partidul Social-Democrat—PSD) of Romania since May 2021. The co-author Dragoș Tudorașcu-Dobre has been, between March 2020 and August 2021, a dues-paying member of the Party of Liberty, Unity and Solidarity (Partidul Libertate, Unitate și Solidaritate—PLUS), which was in an electoral alliance with the Save Romania Union party (Uniunea Salvați România—USR), followed by their merger in April 2021.

Data Availability

Data are available here: https://drive.google.com/drive/folders/1DFNDYNMJf6lGwnNCx6FxoqHuK_qc3RMV

LLMs Disclosure

The authors would like to acknowledge the use of Perplexity AI, Consensus, and ChatGPT assistants as tools for bibliographic research and literature review, for structuring the article, and for grammar and style improvement during the preparation of this article. All sources cited were subsequently verified for accuracy and relevance by the authors.

Supplementary Material

Supplementary material for this article is available online in the format provided by the author (unedited).

References

Abualigah, L., Khaleel, N., Omari, M., Abd Elaziz, M. E., & Gandomi, A. H. (2021). Survey on Twitter sentiment analysis: Architecture, classifications, and challenges. In V. Kadyan, A. Singh, M. Mittal, & L. Abualigah (Eds.), *Deep learning approaches for spoken and natural language processing* (pp. 1–18). Springer Nature. https://doi.org/10.1007/978-3-030-79778-2_1

Albayati, M., & Altamimi, A. (2019a). Identifying fake Facebook profiles using data mining techniques. *Journal of ICT Research and Applications*, *13*(2), 107–117. https://doi.org/10.5614/itbj.ict.res.appl.2019.13.2.2

Albayati, M., & Altamimi, A. (2019b). MDFP: A machine learning model for detecting fake Facebook profiles using supervised and unsupervised mining techniques. *International Journal of Simulation: Systems, Science & Technology*, *20*(1), 1–10. https://doi.org/10.5013/IJSSST.a.20.01.11

Aljabri, M., Zagrouba, R., Shaahid, A., Alnasser, F., Saleh, A., & Alomari, A. M. (2023). Machine learning-based social media bot detection: A comprehensive literature review. *Social Network Analysis and Mining*, *13*(20), 1–40. https://doi.org/10.1007/s13278-022-01020-5

Arega, K. L., Alasadi, M. K., Yaseen, A. J., Salau, A. O., Braide, S. L., & Bandele, J. O. (2023). Machine learning based detection of fake Facebook profiles in Afan Oromo language. *Mathematical Modelling of Engineering Problems*, *10*(6), 1987–1993.

Autoritatea Electorală Permanentă. (2019). *Legislatie Electorala (Legea nr. 33/2007 privind organizarea şi desfăşurarea alegerilor pentru Parlamentul European, republicată, cu modificările şi completările ulterioare—Text actualizat)*. Parlamentul României.

Avaaz. (2019). *Far right networks of deception: Avaaz investigation uncovers food of disinformation, triggering* *shutdown of Facebook pages with over 500 million views ahead of EU elections*. https://s3.amazonaws.com/avaazimages.avaaz.org/Networks_Report_Update_Page_July_2019.pdf

Azami, P., & Passi, K. (2024). Detecting fake accounts on Instagram using machine learning and hybrid optimization algorithms. *Algorithms*, *17*(10), 2–19. https://doi.org/10.3390/a17100425

Azzaakiyyah, H. K. (2023). The impact of social media use on social interaction in contemporary society. *Technology and Society Perspectives (TACIT)*, *1*(1), 1–9. https://doi.org/10.61100/tacit.v1i1.33

Beer, D. (2020). The social power of algorithms. In D. Beer (Ed.), *The social power of algorithms* (pp. 1–13). Routledge.

Boshmaf, Y., Logothetis, D., Siganos, G., Lería, J., Lorenzo, J., Ripeanu, M., Beznosov, K., & Halawa, H. (2016). Íntegro: Leveraging victim prediction for robust fake account detection in large scale OSNs. *Computers & Security*, *61*, 142–168, https://doi.org/10.1016/j.cose.2016.05.005

Bradshaw, S., Bailey, H., & Howard, P. N. (2020). *Industrialized disinformation: 2020 global inventory of organized social media manipulation*. Oxford Internet Institute.

Bradshaw, S., & Howard, P. N. (2017). *Troops, trolls and troublemakers: A global inventory of organized social media manipulation*. Oxford Internet Institute.

Bradshaw, S., & Howard, P. N. (2019). *The global disinformation order: 2019 global inventory of organised social media manipulation*. Oxford Internet Institute.

Bundesministerium der Justiz. (2017). *Gesetz zur Verbesserung der Rechtsdurchsetzung in sozialen Netzwerken (Netzwerkdurchsetzungsgesetz—NetzDG).* https://www.gesetze-im-internet.de/netzdg/BJNR335210017.html

Casero-Ripollés, A., Alonso-Muñoz, L., & Moret-Soler, D. (2025). Spreading false content in political campaigns: Disinformation in the 2024 European Parliament elections. *Media and Communication*, *13*, Article 9525. https://doi.org/10.17645/mac.9525

Centrul de Sociologie Urbană și Regională. (2024). *Sondaj de opinie la nivel național: Ianuarie 2025*. https://curs.ro/wp-content/uploads/2024/01/Prezentare-sondaj-national-ianuarie-2024.pdf

Corbu, N., Bârgăoanu, A., Durach, F., & Ștefăniță, O. (2022). Predictors of engagement on social media and instant messaging platforms during the Covid-19 pandemic: Evidence from Romania. *Romanian Journal of Communication and Public Relations*, *24*(57), 7–23.

Corzo, H. (2021, October 20). Why understanding engagement is a key part of earned media measurement. *NewsWhip*. https://www.newswhip.com/2021/10/engagement-earned-media-measurement

DataReportal. (n.d.). *Global social media statistics*. https://datareportal.com/social-media-users

Durach, F., Ciocea, M., & Nastasiu, C. (2025). Countering disinformation: A delicate balance between international action and national particularities. *Media and Communication*, *13*, Article 9529. https://doi.org/10.17645/mac.9529

Elyusufi, Y., Elyusufi, Z., & Kbir, M. A. (2019). Social networks fake profiles detection based on account setting and activity. In B. A. Mohamed, İ. R. Karaşo, R. Saadane, W. Mtalaa, & B. A. Abdelhakim (Eds.), *Proceedings of the 4th International Conference on Smart City Applications* (Article 37). ACM. https://doi.org/10.1145/3368756.3369015

European Commission. (n.d.). *Strategic communication and countering foreign information manipulation and interference*. https://commission.europa.eu/topics/countering-information-manipulation_en

European Commission. (2022). *2022 Strengthened code of practice on disinformation*. https://digital-strategy.ec.europa.eu/en/library/2022-strengthened-code-practice-disinformation

European Commission. (2023). *Flash Eurobarometer 522—Democracy*. https://europa.eu/eurobarometer/surveys/detail/2966

European Commission. (2024). *Standard Eurobarometer 102—Media use in the European Union* (Eurobarometer Report: October–November 2024). https://europa.eu/eurobarometer/surveys/detail/3215

European Commission. (2025). *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: Report on the 2024 elections to the European Parliament* (SWD(2025) 147 final). https://commission.europa.eu/document/download/2a7fddb2-e927-4079-92cc-4bb4279e9a46_en

European Digital Media Observatory Task Force. (2024). *Final report: Outputs and outcomes of a community-wide effort*. European Digital Media Observatory. https://edmo.eu/wp-content/uploads/2024/07/Final-Report-%E2%80%93-EDMO-TF-EU24.pdf

European External Action Service. (2024). *2nd EEAS report on foreign information manipulation and interference threats a framework for networked defence*. European Commission.

European External Action Service. (2025). *3rd EEAS report on foreign information manipulation and interference threats exposing the architecture of FIMI operations*. European Commission.

European Parliament. (2024). *National results: Romania—2024–2029*. https://results.elections.europa.eu/en/national-results/romania/2024-2029

Ferrara, E., Varol, O., Davis, C., Menczer, F., & Flammini, A. (2016). The rise of social bots. *Communications of the ACM*, *59*(7), 96–104. https://doi.org/10.1145/2818717

Gherghel, I.-V. (2009). *Forme de manipulare televizuală*. Editura Limes.

Giglietto, F., Righetti, N., Rossi, L., & Marino, G. (2020). It takes a village to manipulate the media: coordinated link sharing behavior during 2018 and 2019 Italian elections. *Information, Communication & Society*, *23*(6), 867–891. https://doi.org/10.1080/1369118X.2020.1739732

Gotfredsen, S. G., & Dowling, K. (2024, July 9). Meta is getting rid of CrowdTangle—and its replacement isn't as transparent or accessible. *Columbia Journalism Review*. https://www.cjr.org/tow_center/meta-is-getting-rid-of-crowdtangle.php

Graham, T., Hames, S., & Alpert, E. (2024). The coordination network toolkit: A framework for detecting and analysing coordinated behaviour on social media. *Journal of Computational Social Science*, *7*, 1139–1160. https://doi.org/10.1007/s42001-024-00260-z

Gruzd, A., Mai, P., & Soares, F. B. (2022). How coordinated link sharing behavior and partisans' narrative framing fan the spread of Covid-19 misinformation and conspiracy theories. *Social Network Analysis and Mining*, *12*(118), 1–12. https://doi.org/10.1007/s13278-022-00948-y

Gupta, A., & Kaushal, R. (2017). Towards detecting fake user accounts in Facebook. In Dhiren Patel (Ed.), *2017 ISEA Asia security and privacy (ISEASP)* (pp. 1–6). IEEE. https://doi.org/10.1109/ISEASP.2017.7976996

Hakimi, A., Ramli, S., Wook, M., Zainudin, N., Hasbullah, N., Wahab, N., & Afiza, M. (2019). Identifying fake account in Facebook using machine learning. In H. Badioze Zaman, A. F. Smeaton, T. K. Shih, S. Velastin, T. Terutoshi, N. Mohamad Ali, & M. Nazir Ahmad (Eds.), *Advances in visual informatics* (pp. 441–450). Springer. https://doi.org/10.1007/978-3-030-34032-2_39

Hothman, T. (2019, August 21). Goodbye Netvizz :(…. *Tristan Hotham*. https://tristanhotham.com/2019/08/21/goodbye-netvizz

Howard, P. N., Woolley, S., & Calo, R. (2018). Algorithms, bots, and political communication in the US 2016 election: The challenge of automated political communication for election law and administration. *Journal of Information Technology & Politics*, *15*(2), 81–93. https://doi.org/10.1080/19331681.2018.1448735

Huang, Z., & Liu, D. (2024). *Economics of social media fake accounts*. SSRN. https://doi.org/10.2139/ssrn.4206104

Imperva. (2019). *Bad bot report 2019: The bot arms race continues*. https://www.imperva.com/resources/resource-library/reports/2019-bad-bot-report

Imperva. (2024). *2024 bad bot report*. https://www.imperva.com/resources/resource-library/reports/2024-bad-bot-report-report-ty?lang=EN&asset_id=6912&gated=1

Imperva. (2025). *2025 Imperva Bad Bot Report. The Rapid Rise of Bots and the Unseen Risk for Business*. https://www.imperva.com/resources/resource-library/reports/2025-bad-bot-report

Institutul Român pentru Evaluare și Strategie. (2024). *Românii în anul 2024*. https://ires.ro/uploads/articole/ires_bilantul-anului-2024_sondaj-national.pdf

Jadhav, G., Patel, K., & Gawande, R. (2021). Detecting fake accounts on social media using neural network. *International Journal of Creative Research Thoughts (IJCRT)*, *9*(11), 56–58.

Johnston, K. A., & Lane, A. B. (2019). An authenticity matrix for community engagement. *Public Relations Review*, *45*(4), Article 101811. https://doi.org/10.1016/j.pubrev.2019.101811

Katzenbach, C., & Ulbricht, L. (2019). Algorithmic governance. *Internet Policy Review*, *8*(4), 1–18. https://doi.org/10.14763/2019.4.1424

Khaled, S., El-Tazi, N., & Mokhtar, H. M. O. (2018). Detecting fake accounts on social media. In N. Abe, H. Liu, C. Pu, X. Hu, N. Ahmed, M. Qiao, Y. Song, D. Kossmann, B. Liu, K. Lee, J. Tang, J. He, J. & Saltz (Eds.), *IEEE international conference on big data (big data)* (pp. 3672–3681). IEEE. https://doi.org/10.1109/BigData.2018.8621913

Kushner, S. (2013). The freelance translation machine: Algorithmic culture and the invisible industry. *New Media & Society*, *15*(8), 1241–1258. https://doi.org/10.1177/1461444812469597

Lilkov, D. (2019). *European Parliament elections: The disinformation challenge*. Wilfried Martens Centre for European Studies. https://www.martenscentre.eu/wp-content/uploads/2020/06/european-elections-disinformation.pdf

Litt, E., Zhao, S., Kraut, R., & Burke, M. (2020). What are meaningful social interactions in today's media landscape? A Cross-Cultural Survey. *Social Media + Society*, *6*(3). https://doi.org/10.1177/2056305120942888

Meta. (n.d.-a). *Community standards*. https://transparency.meta.com/policies/community-standards

Meta. (n.d.-b). *Fake accounts*. https://transparency.meta.com/reports/community-standards-enforcement/fake-accounts/facebook

Meta. (n.d.-c). *Inauthentic behavior*. https://transparency.meta.com/en-us/policies/community-standards/inauthentic-behavior

Meta. (2025). *Meta content library and API*. https://transparency.meta.com/ro-ro/researchtools/meta-content-library

Michael, K. (2017). Bots trending now: Disinformation and calculated manipulation of the masses [Editorial]. *IEEE Technology and Society Magazine*, *36*(2), 6–11. https://doi.org/10.1109/MTS.2017.2697067

Ministry of Education. (2022). *Ordin nr. 4800 din 26 august 2022 privind aprobarea programelor şcolare din categoria curriculum la decizia şcolii, nivel liceal, elaborate în cadrul proiectului sistemic Profesionalizarea carierei didactice—PROF—POCU/904/6/25/Operaţiune compozită OS 6.5, 6.6, cod SMIS 146587, al cărui beneficiar este Ministerul Educaţiei*. Government of Romania. https://rocnee.eu/images/rocnee/fisiere/programe_scolare/OME_4800_2022_si_ANEXE_1_2_3_CDS.pdf

Molleda, J. C. (2010). Authenticity and the construct's dimensions in public relations and communication research. *Journal of Communication Management*, *14*(3), 223–236.

Moore, M. (2023). Fake accounts on social media, epistemic uncertainty and the need for an independent auditing of accounts. *Internet Policy Review*, *12*(1). https://doi.org/10.14763/2023.1.1680

Mughaid, A., Obeidat, I., Alzu'bi, S., Elsoud, E., Alnajjar, A., Alsoud, A., & Abualigah, L. (2023). A novel machine learning and face recognition technique for fake accounts detection system on cyber social networks. *Multimedia Tools and Applications*, *82*, 26353–26378. https://doi.org/10.1007/s11042-023-14347-8

Navarro, J. T., García, L. B., & Oleart, A. (2025). How the EU counters disinformation: Journalistic and regulatory responses. *Media and Communication*, *13*, Article 10551. https://www.cogitatiopress.com/mediaandcommunication/article/view/10551

Omar, A. S., & Ondimu, K. O. (2024). The impact of social media on society: A systematic literature review. *The International Journal of Engineering and Science*, *13*(6), 96–106. https://shorturl.at/ga68c

Oprea, B. (2022). *Fake news și dezinformare online: recunoaște și verifică: Manual pentru toți utilizatorii de internet* (2nd ed.). Editura Polirom.

Oprea, B. (2023). Use of Facebook accounts with inauthentic behavior in elections: The Romanian presidential election case. *Romanian Journal of Communication and Public Relations*, *25*(3), 53–72.

Oprea, B. (2024). Matricea autenticității, instrument de detectare a conturilor de Facebook cu comportament neautentic. In F. Ardelean & I. Laza (Eds.), *Mass-media, sub lupa cercetătorilor și a practicienilor* (pp. 397–416). Tritonic Books; Editura Universității din Oradea.

Padmavathi, A., & Vaisshnavi, K. B. (2024). Comparative analysis of fake account detection using machine learning algorithms. In B. Roy (Ed.), *2024 4th International conference on artificial intelligence and signal processing (AISP)* (pp. 1–7). IEEE. https://doi.org/10.1109/AISP61711.2024.10870733

Pamment, J., Nothhaft, H., Agardh-Twetman, H., & Fjällhed, A. (2018). *Countering information influence activities: The state of the art* (version 1.4). Lund University. https://rib.msb.se/filer/pdf/28697.pdf

Papakyriakopoulos, O., Medina Serrano, J. C., & Hegelich, S. (2020). Political communication on social media: A tale of hyperactive users and bias in recommender systems. *Online Social Networks and Media*, *15*, Article 100058. https://doi.org/10.1016/j.osnem.2019.100058

Parliament of Australia. (2019). *Criminal code amendment (sharing of abhorrent violent material) bill 2019*. https://www.aph.gov.au/Parliamentary_Business/Bills_Legislation/Bills_Search_Results/Result?bId=s1201

Pasieka, N., Kulynych, M., Chupakhina, S., Romanyshyn, Y., & Pasieka, M. (2021). Harmful effects of fake social media accounts and learning platforms. In V. Buriachok, D. Ageyev, V. Lahno, & V. Sokolov (Eds.), *CEUR workshop proceedings* (Vol. 2923, pp. 252–259). CEUR-WS. https://ceur-ws.org/Vol-2923/paper28.pdf

Programul de Educație Media, bilanț la final de an școlar: Peste 50.000 de elevi mai bine pregătiți să recunoască dezinformarea. (2025, June 26). *Centrul pentru Jurnalism Independent*. https://cji.ro/programul-de-educatie-media-bilant-la-final-de-an-scolar-peste-50-000-de-elevi-mai-bine-pregatiti-sa-recunoasca-dezinformarea

Radu, R.-N. (2025). Romania. In N. Newman, A. R. Arguedas, C. T. Robertson, R. Kleis Nielsen, & R. Fletcher (Eds.), *Reuters Institute digital news report 2025* (pp. 102–103). Reuters Institute for the Study of Journalism; University of Oxford. https://doi.org/10.60625/risj-8qqf-jt36

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) (Text with EEA relevance). *Official Journal of the European Union*, L 277/1. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022R2065

Rodenhäuser, T. (2023). The legal boundaries of (digital) information or psychological operations under international humanitarian law. *International Law Study*, *100*, 541–573.

Romanov, A., Semenov, A., Mazhelis, O., & Veijalainen, J. (2017). Detection of fake profiles in social media: Literature review. In T. A. Majchrzak, P. Traverso, K.-H. Krempels, & V. Monfort (Eds.), *Proceedings of the 13th International Conference on Web Information Systems and Technologies* (WEBIST 2017) (pp. 363–369). SciTePress. https://doi.org/10.5220/0006362103630369

Samoilenko, S. A. (2017). Strategic deception in the age of 'truthiness.' In I. Chiluwa (Ed.), *Deception and* *deceptive communication: Motivations, recognition techniques and behavioral control* (pp. 1–19). Nova Science Publishers.

Schultz, A. (2019). *How does Facebook measure fake accounts?* Meta. https://about.fb.com/news/2019/05/fake-accounts

Scott, M. (2019, May 23). Europe's failure on 'fake news.' *Politico*. https://www.politico.eu/article/europe-elections-fake-news-facebook-russia-disinformation-twitter-hate-speech

Toma, B., & Suciu, C. (2024). *Țintele dezinformării pe teme europene în anul electoral 2024*. Centrul Român de Politici Europene. https://www.crpe.ro/wp-content/uploads/2024/10/CRPE-Disinformation-2024-Raport-complet.pdf

Tunç, Ü., Atalar, E., Gargı, M. S., & Ergül Aydın, Z. (2024). Classification of fake, bot, and real accounts on Instagram using machine learning. *Journal of Polytechnic*, *27*(2), 479–488. https://dergipark.org.tr/en/pub/politeknik/issue/83819/1136226

Voitovych, O., Kupershtein, L., Kupershtein, L., & Holovenko, V. (2022). Detection of fake news accounts in social media. *Cybersecurity: Education, Science, Technique*, *2*(18), 86–98. https://doi.org/10.28925/2663-4023.2022.18.8698

Walker, S., Mercea, D., & Bastos, M. (2019). The disinformation landscape and the lockdown of social platforms. *Information, Communication & Society*, *20*(11), 1531–1543. https://doi.org/10.1080/1369118X.2019.1648536

we are social, & Meltwater. (2025). *Digital 2025: Global overview report*. DataReportal. https://datareportal.com/reports/digital-2025-global-overview-report

Weedon, J., Nuland, W., & Stamos, A. (2017). *Information operations and Facebook*. Facebook. https://i2.res.24o.it/pdf2010/Editrice/ILSOLE24ORE/ILSOLE24ORE/Online/_Oggetti_Embedded/Documenti/2017/04/28/facebook-and-information-operations-v1.pdf

World Bank Group. (2025). *Population, total*. https://data.worldbank.org/indicator/SP.POP.TOTL

X. (2025). *Rules and policies*. https://help.x.com/en/rules-and-policies

Zhang, Y., Wells, C., Wang, S., & Rohe, K. (2018). Attention and amplification in the hybrid media system: The composition and activity of Donald Trump's Twitter following during the 2016 presidential election. *New Media & Society*, *20*(9), 3161–3182. https://doi.org/10.1177/1461444817744390

About the Authors

Bogdan Oprea has a PhD in the manipulation on social media and teaches the study of disinformation and manipulation at BA and MA levels. With more than 25 years of experience in journalism and communication in public administration, he has given more than 100 lectures, courses, etc., in about 20 countries.

Paula Pașnicu is an MA student in communication campaigns in advertising and public relations at the Faculty of Journalism and Communication Studies–University of Bucharest. She holds a journalism BA, with a thesis on televised disinformation. Her academic interests include media manipulation, online disinformation, political communication, and electoral influence.

Alexandru-Ninel Niculae is an MA student in communication campaigns at the University of Bucharest. He holds a journalism BA, with a thesis on online manipulation. With a TV reporting experience, his research interests include media manipulation, disinformation, political communication, and strategies of electoral influence.

Constantin-Cozmin Bonciu is a graduate of the University of Bucharest in communication and public relations, working in the IT industry, where he combines strong communication skills with a passion for technology. He is driven by innovation and enjoys exploring how tech can improve both business and everyday life.

Dragoș Tudorașcu-Dobre is a social work BA graduate and a journalism student at the University of Bucharest. He has worked with NGOs focused on social work and has experience as a TV news writer. His interests include workers' rights and the propaganda and disinformation of the digital age.