

DIGITAL POLITICAL CAMPAIGNING: CONTEMPORARY CHALLENGES AND REGULATION

Gabriela Borz, University of Strathclyde, Glasgow, UK and Babes-Bolyai University, Cluj-Napoca, Romania.

Fabrizio de Francesco, University of Strathclyde, Glasgow, UK

Abstract

How can multiple organisational, social and political actors effectively address the contemporary challenges of digital political campaigning? We proceed by reviewing the increased theoretical and empirical importance of digital political campaigning. We discuss the new research advances in the field and acknowledge the necessity for interdisciplinary research given the rapidly evolving techniques and the imminent positive and negative risks of digital campaigning. We present a multi-level actor approach for dealing with the risks of digital political campaigning. We outline the contribution of this issue and identify relevant gaps for future research.

Keywords: digital political campaigning, risk, platforms, regulation, political parties

Elections play an important role in legitimising the system in both democratic and non-democratic states. Whilst input legitimacy is achieved through citizens' participation in elections, referenda, citizens assembly, throughput legitimacy is about efficacy in the process of decision making and output legitimacy concerns the outcomes, policy benefits to citizens (Schmidt, 2013; Schmidt and Wood, 2019). Digital technologies have transformed all these processes related to legitimacy. We encounter digital technologies at all stages in the electoral cycle. Digital technologies are used in campaign strategies and campaign content, management of data in electoral registers, use of voter personality data for targeting use of AI generated materials for manipulating voters. Citizen electoral participation and consequently input legitimacy may be positively or negatively impacted by these technologies. Henceforth, the electoral management and its integrity is an important aspect of a democratic political system (Garnett and James, 2020). Electoral integrity and electoral malpractice become important concepts in the process of throughput legitimacy in the digital era. As legitimacy is linked to values, rights and the institutional realization of those rights, political structures need to reflect socially accepted values in order to be perceived as legitimate. Diffuse support for the system can then happen when voters trust the electoral processes (Banducci and Karpp 2003). Conversely, a legitimacy crisis appears when there is a mismatch between structures and values (Bolleyer and Rech, 2012) or more specifically, between voters expectation of integrity and malpractice in electoral management processes.

In this paper we focus our attention on the pre-election period, more specifically campaigning in the on-line environment. As digital campaigning gains more global political and financial significance so does the importance attributed to various positive but also negative effects generated by its use. Input legitimacy can increase if turnout and citizen participation is augmented by digital technologies. Output legitimacy can increase if regulation, co-regulation and self-regulation at multiple levels will address all these concerns. In this context, digital

technologies have the potential to either increase the legitimacy crisis or act as opportunities for promoting democratic values.

The growing relevance of digital political campaigning and its associated risks

Digital political campaigning is becoming a topical issue mainly due to the perceived *negative risks* it generates (Jaurisch 2021). In political, philosophical and economics frameworks, risk is mainly seen as “the probability of the occurrence of a negative outcome” (Ferretti, 2016: 3) or more specifically ‘risk equals hazard times exposure’ (Chicken and Posner 1998: 7) with hazard being the thing or situation that can cause harm. In the context of digital electoral governance, we understand risks as the consequences of specific activities undertaken during digital political campaigning. Various digital campaign activities such as microtargeting, use of personal data, personality tailored messages, AI generated messages and videos contribute to increasing the probability of risks for individual, political and organisational actors involved in the process of deciding, producing, disseminating or consuming the digital political message. Both legitimate and illegitimate activities take place in the course of this process. Amongst the latter is the foreign influence in national elections which has already raised various alarm bells (Ringhand 2021) and produces systemic risks in the form of manipulation of electoral results (Tenove et al. 2018) which undermine democratic principles and generate political instability.

The *type of risk* depends on the actor which we consider as main reference: political parties, consultancies, on-line platforms, citizens or democratic establishments. We acknowledge the probability of both positive and negative risks (Klinke and Renn 2021: 544) resulting from activities of digital political campaigning. Among the *negative risks* generated by digital campaigning and relevant for citizens in a representative democracy we can list distorted debates, inequality of participation in political discussions, polarization, lack of public scrutiny, lack of privacy, transparency, manipulation, disinformation, misinformation, malinformation. Disinformation in particular, is considered the number one global risk in 2024 according to the World Economic Forum risk perception survey (The World Economic Forum, 2024). Disinformation in the context of digital campaigning has itself harmful implications not only for consumers as potential voters, but also for the individuals delivering the digital message. The digital labour involved in its implementation may be precarious, run by disinformation farms based in grey/illicit digital economies across the globe (Grohman and Ong 2024). The agencies targeting the opposition parties may be paid by the incumbent parties and could be also protected from legal prosecution by the latter (George 2019, Ong 2020). Moreover, disinformation may be AI generated and more convincing than human generated disinformation (Spitale et al. 2023). Negative risks relevant for political parties include the potential of being perceived as a single issue party by voters due to the granularity inherent to microtargeting techniques (Zuiderveen et al 2018), while the negative risks of on-line platforms include, for example, reputation and liability risk (Gaultier-Gaillard and Louisot, 2006).

In addition to the negative effects, we also acknowledge the list of potential *positive risks* (benefits) across multi-level actors. The positive implications of digital political campaigning (Galais and Cardenal 2017) for political parties relate to higher fortunes in elections, reaching out to a wider audience sometime, low cost (Dobber et al. 2022), better engagement with

remote users who could not get access to traditional campaigning or the strengthening of partisan identities (Lavigne, 2021). At the individual level positive risks relate to increased interest in politics (Mathes et al. 2022), higher (digital) political engagement, potential for high(er) turnout in elections, referenda etc. At the system level one could expect a higher quality of democracy with high levels of citizen (digital) participation in politics, higher satisfaction with democracy. Many of these risks are still to be empirically tested.

Regulation as a response to risks generated by digital campaigning

The development of digital campaigning as a tool already acknowledged by political parties (Almodt 2024) and the global spread of microtargeting (Votta et al. 2024) generates regulatory challenges for policy makers but also organisational, behavioural and attitudinal changes for consumers and promoters of digital (political) campaigning. How digital political campaigning is regulated at various levels has implications for democratic principles, political behaviour and subsequent policies adopted. Risks can hence be effectively managed through the adoption of relevant regulation or self-regulation at each level.

National governments and international organisations alike started taking small steps towards addressing the positive and negative effects of digital campaigning (Mitrea 2024). For example, over the past decade the European Union has adopted a combination of soft and hard laws (Longhini, 2024) which has culminated in 2024 with the adoption of the Code of Conduct for the 2024 European Parliament Elections (European Commission 2024a) and the Guidelines on the mitigation of systemic risks for electoral processes (European Commission 2024b) ahead of European elections. This followed from previous initiatives such as Defence of Democracy package (European Commission, 2023) and The European Democracy Action Plan (European Commission, 2020) which had as aim the empowerment of democracies by promoting free and fair elections, countering disinformation, media freedom, pluralism.¹

The policy response to the challenges of on-line political campaigning require discussion at all levels (international organisations, national governments, digital platforms, political parties and their members, and individual voters). What are the implications of digital political campaigning at the individual (citizens and voters), organisational (political parties), national (governments) and trans-national (European Union) institutional level? To what extent are these implications distinct from traditional electoral campaigning? And does this divergence trigger policy responses forming a new mode of regulatory governance distinctive from existing legislation governing political campaigning?

To answer these questions, we consider digital political campaigning as a contemporary evolving way of conducting electoral politics in the on-line environment with the help of digital technologies. The process complements traditional forms of political campaigning and digital activities available in the 1990s (Tan: 2020, Kumar: 2022). The process still involves the preparation, promotion, communication and dissemination of electoral messages with the ultimate aim of gaining votes, but in the on-line environment, on a larger scale in terms of audience and communication frequency. The use of on-line portals, webpages, on-line

¹ For an overview of EU and national laws related to digital campaigning see the DIGIEFFECT Data visuals available at: <https://digieffect.eu/data-visuals/>.

platforms within and outside the electoral cycle can hence increase in the number of campaign activities, the number of actors involved at all stages of campaigning (Koc-Michalska et al. 2023: 256), the required financial resources and the amount of personal data manipulated in the process. Ultimately these push the time frame outside the dedicated legal time for campaigning. Strong supervisory (independent) bodies are needed to be sure that on-line adverts are not posted in the pre-electoral period, especially when the scale of on-line adverts exceeds the international and national monitoring capacity.

Conceptual clarifications and current interdisciplinary theoretical advancements

In this rapidly evolving field, political behaviour and communication approaches have defined electoral campaigning in the on-line environment as either *digital campaigning* (Jungherr 2016: 359, 360; Kim et al. 2018: 23; Koc-Michalska et al. 2023: 256, Vanden Eynde and Maddens 2023: 2) or *data-driven campaigning* (Brkan 2022: 350, 351; Dommet et al 2024: 13; Kefford et al. 2023: 449; Dommet, Kefford and Kruschinski 2024). The recent advances perform very well at identifying the specific campaign activities such as data processing or the actors involved in digital campaigning and some effects of the process. However, the literature lacks comprehensive comparative accounts on how to address the effects of digital campaigning.

Very few studies (Garnett and James, 2020; Brkan 2022) remark the similarities with market consumer behaviour strategies, in the form of personal data processing for commercial targeted advertising. A comprehensive approach to digital political campaigning should nevertheless address the risks associated with the content of the message, its preparation and dissemination techniques. We already know that electoral malpractice (Birch, 2011) can take the form of manipulation of vote preference formation and expression, and manipulation of the voting process. With the use of digital technologies however, it is the volume, the content, the targeted computational distribution and the covered intent of personal data management that can potentially manipulate the opinion of voters and influence their electoral behaviour.

We argue that a risk governance approach to digital political campaigning takes into account not only the multitude of actors and activities involved in the process but also the content of the message and more importantly, its implications for political parties, for citizens as audience, for the third-parties and ultimately for elections and the political system overall (Borz et al. 2024). A risk governance approach encompasses not only the actors but also their regulatory and organizational decisions adopted as a response to the positive and negative risks.

With very few exceptions related to systemic risks only and their moderation in electoral management processes (Micova and Schnurr 2024, Vincent et al 2021), the literature lacks a risk approach to digital political campaigning at multiple levels. On similar lines with public interest perspectives (Olson 1971), a risk approach also justifies the regulation of digital campaigning on the basis of reducing the risk of information asymmetry between policymakers and citizens, on the one hand, and digital and social media platforms, on the other. However, any regulatory intervention in this sector is characterised by a high-level of political uncertainty related to the dynamism of tech and social media companies. This issue

magnifies the risk of errors and unintended consequence of the design of regulatory responses for governing disruptive technologies (such as the risk of overregulation).

Most scholarly advances specifically related to digital political campaigning are from political science (electoral integrity, political behaviour, regulation and party organisation), communication studies (public sphere, affective polarisation), legal studies (human rights), psychology (personality related studies) or international relations (security threats).

Comparative politics studies on party organisation emphasize that centralized, professional parties which have previously replaced mass parties (Farrell and Webb 2002), have also adapted to the technological advancements (Sandri et al 2024) and notwithstanding the potential dangers, they could make use of AI to monitor and apply democratic processes inside the party (Novelli et al. 2024). Parties move from campaign organisers in the traditional environment to the campaign organisers in the digital environment and increasingly digitize their activities (Barberà et al 2024). Studies on the impact of digital campaigning on political behaviour are relatively scarce and more comparative evidence is necessary. Haenschen (2023) found little evidence of Facebook adverts on turnout in the American context but Dobber et al. (2021), Endres (2019) found that partisans' attitudes can be negatively affected by a microtargeted deepfake message about single candidates.

Recent research in political psychology tests the negative impact of personality tailored ads on voting behaviour. Not only that individuals find personality tailored adverts created by generative AI more convincing, but to a small margin, these adverts can impact on voting decision (Simchon et al. 2024). Political behaviour studies already show that citizens reject targeting based on individual characteristic (Vliegenthart et al 2024) and increase their cynicism about elections if their perceptions about being exposed to false information increases (Jones-Jang et al. 2021). The problem that still needs resolving, through regulatory and educational means, is the empowerment of citizens with the digital skills necessary for detecting the hazardous content spread via digital microtargeting.

The international relations scholarship related to digital campaigning discusses the topic in the context of security studies due to the cyber threats and possibility of foreign interference in elections (Buchanan 2020). Kruck and Weiss (2023) talk about the regulatory security state, while other scholars argue that 'there is not only more regulation in security, there is more security in regulation (Mügge 2023: 1431), meaning that at the system level security logics invade the domain of technology regulation. In this context we can justify national regulation pertaining to digital campaigning as a response to a systemic risks such as threats to national security.

Political communication theorists (Jungherr 2023, Jungherr and Schroeder 2023) emphasize the negative impact of AI on the public arena functions. In addition to risks such as mechanical reinforcement of societal biases, algorithmic deployment of adverts that skew information flows or the low number of companies providing AI-based applications and services, they express concerns over the rise of intermediary digital media structures which impact on the development of publics and the ability of society to see a reflection of itself. Moreover, the impact of AI on democracy is associated with the electoral process. Future scholarship

however should provide a detailed account of the impact of digital political campaigning on all democratic principles across types of democracy.

Lastly, legal advances in the field of digital law with connection to digital campaigning talks about a digital justice gap and the right to an effective remedy in a less fragmented regulatory environment (Rabinovich-Einy and Katsh 2017, De Gregorio 2022). Algorithmic discrimination for individuals and communities during digital campaigning for example, is in need for effective remedies, or, in other words, effective regulatory measures.

Aims of the special issue

This special issue aims to unpack the reactions of all actors involved in the process of digital political campaigning. We explore how party members get involved in the process of digital campaigning and how the latter impacts on the process of political engagement. We aim to uncover 1) what risk prompts the regulation of digital political campaigning at the international and national level; 2) the object of digital regulation at the international and national level and also the missing aspects of such regulation 3) the organisational changes prompted by digital campaigning 4) how the subjects of such regulation react to it.

In particular, this special issue presents the challenges of political digital campaigning for the diffusion of information and for democracy, the principles which should inform the regulation of digital campaigning, introduces indicators for the way in which such regulation should be evaluated and maps the responses to the digital regulatory regimes introduced. We aim to discuss and integrate the regulatory responses to the issue of digital campaigning at all levels starting with international organisation, national governments, digital platforms (such as Facebook (Meta), Twitter, Microsoft and Mozilla), political parties and party members.

At the organisational level we observe digital platforms such as Google, X (Twitter) and Facebook (Meta) and national political parties and at the individual level, we focus on party members and party activists behaviour and activities. Which level of party organisation implements digital campaigning and with what funds? At the national and international level we assess EU and national regulatory frameworks. How effective is the national and transnational regulation of digital campaigning? Are digital platforms responsive to national and transnational regulation of digital campaigning? More specifically, the papers discuss how the on-line platforms respond to the regulatory regimes they encounter in this field. At the individual level, we observe party members and sympathisers. Is digital campaigning changing the on-line behaviour of party members and sympathisers? the involvement of party members, activists and supporters in the process of digital campaigning. Finally, this special issue.

The contribution of this special issue

This group of papers makes a clear interdisciplinary contribution to the emerging literature of digital campaign governance. The seven articles of this special issue can be distinguished from the perspectives of digital campaigning and related risks to democracy and pave the way towards normative frameworks for digital electoral campaigns and their specific rules. From an empirical standing point, digital campaigning can be a case study of a broader

phenomenon or can be studied to explore variation in private and public policymakers. On the other hand, empirical analysis can focus on specific elements of digital campaigning such as party policies' electoral funding (either donations or loans) channelled through digital platforms. Another way to zoom in specific elements is to look at specific behaviour of social media actor or pseudo-actors. Finally, causal relationships can be established and tested between digital campaign governance (both as dependent and independent variable) and specific political and institutional conditions.

Gibson et al. (2024) provides a cutting-edge analysis for policy recommendation and a strong empirical contribution by operationalising data driven campaigning. Through an analysis of practices of data-driven campaigning, they provide a conceptual definition of digital campaign regulation which revolving around a set of operational stages of data access, data analysis, and communication to voters. These three stages inform the final stage of decision-making. Each stage is then operationalised in specific indicators for benchmarking. Empirically, they provide a descriptive heat map of the EU regulatory landscape. Ultimately, they recommendations are based on whether the digital campaigning governance is going to be absorbed by later policy sectors or the design of a new regulatory regime. In their conclusion, Gibson et al. indicate a future research avenue in taking seriously data-driven campaigning in the discussion of traditional rules concerning electoral finance and broadcasting. They also pave a way for quantitative analysis possible by collecting data related to their indicators of digital campaign regulation.

In a multidisciplinary fashion combining insights from public policy, European governance and corporate governance, Borz et al. (2024) assess the effectiveness of EU soft law related to digital campaigning. They do so by investigating the variation in the digital platform (i.e., Meta (Facebook), Google, Microsoft, Mozilla, and X(Twitter)) responses to the EU Code of Practice on Disinformation. The compliance of private organisations revolves around voluntary acts, triggered by the need of legitimacy. Their assessment is based on an evaluative framework that follows the behaviour of digital platforms in complying with the code of practice. Accordingly, soft law compliance can be distinguished for the private operators' intention to agree with the principles stated in the code of practices, to formally commit to such principle with a pledge to adopt new procedures and policies, to take compliance actions, and to change the organisational policies and procedures. Through this multi-staged approach to compliance and an analysis of thematic frequencies in the annual reports, they find an asymmetric reporting: most of digital platforms cherry-picked the regulatory issues (transparency, rights and freedom of expression, integrity, empowerment and coordinated responsibility). Contrary to their expectation, symbolic commitment is followed to a certain extent by formal commitment. In other words, symbolic commitment is not a way to elude the soft law compliance as there is a clear association between high level of symbolic commitment and formal commitment expressed in specific pledges of organisational and operational changes. In a similar vein, there is a clear association between levels of commitment and the extent of implemented action for ensuring compliance with the code of practice. Through this content analysis of private corporation reports, they conclude that there is a clear correlation between compliance and ergo regulatory effectiveness and organisational priorities of digital operators. This empirical result points towards the necessity for the European Commission not only to enlarge the soft law's inclusion but also to induce

private market operators of the centrality of the regulatory issues concerning the control of information in digital campaign.

Turning to articles that explored digital campaign regulation as a case study for enhancing our understanding of a broader phenomenon of regulatory governance, from a legal studies perspective, Farrand (2024) provides a discussion of how political advertising on online platforms can be perceived as a threat to democratic legitimacy. This threat—Farrand argues—is not isolated as over the last decades the EU has been particularly vulnerable given the broader geopolitical instability. Specifically, electoral disinformation that is associated with digital and online platforms has been defined by the EU Commission as ‘hybrid threats.’ Provided this conceptual association between digital campaign, online platform and threat, Farrand (2024) argues that it is useful to observe the evolution of the EU digital campaigning regulation through the broader theoretical frameworks of regulatory mercantilism. In such context of vulnerability, this framework explains the shift from a mode of governance (i.e., regulatory capitalism) characterised by the promotion of public-private cooperation to achieve market efficiency, to a stricter public oversight through accountability mechanisms (i.e., regulatory mercantilism) for ensuring security. In the latter regime, regulators seek to promote their own regulatory solutions as international standards to be exported to other polities.

Borucki and Kattemann (2024) examine the German regulatory response to digital campaigning at the platform level, parliamentary parties, national and European level. The authors provide a comparison on the on-line and off-line campaign regulation and find disparities between online and offline regulatory regimes. Their finding is that online regulation is in its early stages. Freedom of expression as expected, is protected by the constitution while online regulations, like NetzDG, focus on removing illegal content, hence addressing disinformation both on the on-line and off-line environment remains on the policy agenda. The Borucki and Kattemann (2024) article also touches upon how platforms regulate themselves and continues with political discussions about campaign governance in party manifestos and parliamentary discourse. Interestingly, they find more discussions about on-line campaign regulation from the side of opposition parties irrespective of the time of the electoral cycle. Contrary to their expectations, the discussion about regulatory changes do not happen with high intensity during the electoral campaigns when one would expect such discussions about changes. The article concludes that huge gaps in the regulation of online campaigning still remain and argue for the necessity of stricter rules.

Rather than using digital campaigning regulation and governance for telling a broader (regulatory) story, several authors of this special issue took the opposite direction: Lupato et al. (2024) use a specific case study of microcredit through online portals—the so-called “digital participatory financing”—to enhance our understanding of how and to what extent digital innovation can influence digitalisation of political parties and, consequently, electoral competition. Through a longitudinal analysis (2015-2021) of the Spanish party Podemos, they clarify what (digital) microcredit means for political parties, explore the consequences of digital microcredit finding that challenger parties use more this digital innovation, and the extent of microcredit is augmented not only by the general expectation of the political party’s success in election but also by the polarised political context. In the last part of their article, relying on the evaluation of the Court of Audits Lupato et al (2024) took a normative stance

by arguing for more and better regulation of these digital funding mechanisms, otherwise the lack of reliability and transparency would deter the mass of political supporter from financing their parties in electoral competition. Accordingly, they article starts from empirical puzzle but ends by providing recommendations for electoral reformers: Clear rules are here required for making a transparent and accountable 'marketplace' of digital financing for political parties especially when engaged in electoral campaigns. Lawmakers and researchers could rely on the approach taken by Gibson et al and Borz et al for mapping the regulatory void of digital participatory financing vis-à-vis traditional form of funding.

In a similar vein, Matuszewski and Szabo (2024) focus on social media virality through hyperactive Twitter accounts to assess their influence on political information diffusion. Through big data analysis, they investigate the influence of hyperactive accounts, defined as 'Twitter handles that follow opinion leaders and disproportionately frequently react to their tweets (respond, retweet, and like them) and participate in discussions about them (mentioning their account names)' (Matuszewski and Szabo 2023: X), on the spread of Polish political (opinion) leaders during the Poland's 2019 European parliamentary election campaign. The big data method allowed them to distinguish between bot-like or human-controlled Twitter accounts. They also observed that social media are not digital agorae where there is an equal participation in the political discussion: Hyperactive Twitter account focalised all the political discussion generated by political opinion leaders throughout the election. Similarly to Lupato et al. (2024), their empirical findings indicate the unintended and negative risks of a specific phenomenon and social behaviour consequent to the ongoing and unstoppable digitalisation.

The flow of information is a key aspect of electoral digitalisation. Rather than explaining the unbalanced distribution between hyperactive and normal social media accounts, Ziegler (2024) focuses on how social media influence organisational capacity of political parties in Germany. Through a quantitative data analysis of a party member panel survey, she was able to observe that digital campaigning is still in its infantile stage of digitalisation as only more organised and professionalised political parties can take full advantage of the positive risks (benefits) that a digital grassroots support in electoral campaign. Similarly to Matuszewski and Szabo (2024), Ziegler (2024) observes that digitalisation of electoral campaigning does not equate with access and high political participation: only senior, male and educated political parties' supporters engage in digital campaigning. Digitalised campaigners tend to be highly engaged with their party routines. Overall, this article is an excellent discussion of the necessity extensive participation of party members in digital campaigning. In her conclusion, she also points out to the more open and democratic nature of digital grassroots vis-à-vis data-driven campaigning. However, the former is more difficult to regulate given the individual responsibility of grass-rooters supporting political parties.

Conclusions

Because digital campaigning cross-cuts different (sub)disciplines such as regulatory governance, political behaviour, political psychology and party politics, public policy, sociology and law, we can group the articles of this special issues in the following clusters. In the first cluster, Borucki and Kattemann (2024), Farrand (2024), Gibson et al. (2024), and Borz et al. (2024) speak to the research community more interested in regulatory governance given

their focus on the behaviour of private market operators. Borz et al. (2024) and Gibson et al. (2024) and propose analytical frameworks for evaluating the regulatory governance of digital campaigning and its unintended (negative) consequences, thus engaging also public policy scholars, lawmakers and practitioners who are searching for model to assess the quality of digital campaigning regulation. Secondly, another cluster of papers that includes Lupato et al. (2024) and Zigler (2024) provides an interesting organisational variation of the parties' capacity to benefit from digitalisation and digital tools. Accordingly, this research strands would be familiar to scholars interested in the organisation of political parties as well as their regulation (especially in the case of Lupato et al. 2023). Connected to this group of paper is the paper by Mautszewski and Szabo (2024) who focused on the relationship between political opinion (and party) leaders and social media users.

A new strand of scholarship should aim to fill in the following gaps at all levels. At the level of individual voter, we need more comparative knowledge about: the exact effect of digital campaigning compared to traditional campaigning, the effect of digital campaigning on political engagement and on voting behaviour and ultimately on the perceived quality of democracy and satisfaction with democracy. We still do not know on a comparative scale, whether digital campaigning, which often complements and 'recycles' the same narratives of broad national-level adverts (Anstead et al., 2018) boosts turnout significantly at the national level. Moreover, does digital campaigning help challenger parties win in elections which are decided by a very low margin? At the country level: governmental actors should consider constitutional and legal changes to address the negative risks. Soft regulation should not be excluded as an option considering its dialog building potential with private market operators. For example, we also need to know more about how individual countries can build regulatory resilience against foreign interference in elections. At the platform level, are global corporations going to comply more with the hard international regulations or will they rather prefer fines and continue with the same operations given that other parties are responsible for the content they deploy on-line during electoral campaigns? At the international level: is it soft regulation or hard regulation more effective at addressing the risks of digital campaigning?

Funding acknowledgement:

The completion of this work was supported by the project “Digital political campaigning: regulatory effectiveness through the eyes of citizens (DIGIEFFECT)” funded by European Union – NextgenerationEU and Romanian Government, under National Recovery and Resilience Plan for Romania, contract no 760035/23.05.2023, cod PNRR-C9-I8-CF CF266/29.11.2022, through the Romanian Ministry of Research, Innovation and Digitalization, within Component 9, Investment I8.

Dr Gabriela Borz is Senior lecturer in Comparative Politics at the University of Strathclyde, Glasgow, United Kingdom. She specializes in the regulation and organization of political parties, EU governance, constitutionalism, corruption. Her most recent project DIGIEFFECT (www.digieffect.eu) investigates the risks associated with digital political campaigning in the European Union.

Dr Fabrizio De Francesco is Senior Lecturer in Public Policy at the School of Government and Public Policy, University of Strathclyde, Glasgow. His research on regulatory institutions, the diffusion of administrative reform, and transnational governance (see his co-edited Elgar Companion to the OECD).

References:

Almodt, R. (2024) Digital campaigning: scope, practice and potential described more by opposition parties across Europe, DIGIEFFECT blog, available at: <https://digieffect.eu/3-digital-campaigning-scope-practice-and-potential-described-more-by-opposition-parties-across-europe/>.

Barberà, G. Sandri, P. Correa, & J. Rodríguez-Teruel (Eds.) (2021) *Digital parties: The challenges of online organisation and participation*. Springer Nature.

Birch, S. (2011) *Electoral malpractice*. Oxford: Oxford University Press.

Borz, G., de Francesco, F., Montgomerie, T. L., & Bellis, M. P. (2024). The EU soft regulation of digital campaigning: regulatory effectiveness through platform compliance to the code of practice on disinformation. *Policy Studies*, 1–21.

<https://doi.org/10.1080/01442872.2024.2302448>

Brkan, M. (2022). The regulation of data-driven political campaigns in the EU: from data protection to specialized regulation. *Yearbook of European Law*, 41, 348-373.

Buchanan, B. D. (2020) *The Hacker and the State: Cyber Attacks and the New Normal of Geopolitics*. Cambridge: Harvard University Press.

Bennet et al. (2018) The democratic interface: Technology, political organization, and diverging patterns of electoral representation. *Information Communication & Society*, 21(11), 1655–1680;

Bolleyer, N. & C. Reh (2012) 'EU legitimacy revisited: the normative foundations of a multilevel polity', *Journal of European Public Policy*, 19:4, 472-490.

Borucki, I., & Kettemann, M. C. (2024). Better safe than sorry? Digital campaigning governance in Germany. *Policy Studies*, 1–23.
<https://doi.org/10.1080/01442872.2024.2311167>

De Gregorio, G. (2022) *Digital Constitutionalism in Europe: Reframing Rights and Powers in the Algorithmic Society* Cambridge: University Press.

Dobber, T., Metoui, N., Trilling, D., Helberger, N., & de Vreese, C. (2021). Do (Microtargeted) Deepfakes Have Real Effects on Political Attitudes? *The International Journal of Press/Politics*, 26(1), 69-91. <https://doi.org/10.1177/1940161220944364>

Dommett, K., Barclay, A., & Gibson, R. (2024). Just what is data-driven campaigning? A systematic review. *Information, Communication & Society*, 27(1), 1–22.
<https://doi.org/10.1080/1369118X.2023.2166794>

Endres Kyle. 2019. "Targeted Issue Messages and Voting Behavior." *American Politics Research* 48:317–28

Election Guide (2024) Democracy Assistance and Election News, available at www.electionguide.org, last accessed April 2024.

European Commission (2020) The European Democracy Action Plan, https://commission.europa.eu/document/63918142-7e4c-41ac-b880-6386df1c4f6c_en
European Commission (2023) Defence of Democracy Package. Available at: https://ec.europa.eu/commission/presscorner/detail/en/ip_23_6453, last Accessed May 2024.

European Commission (2024a) for the 2024 European Parliament Elections Code of Conduct for https://commission.europa.eu/document/bebd9b72-fbb9-42f3-bcea-dbace7e0650f_en, last Accessed May 2024.

European Commission (2024b) Guidelines for providers of Very Large Online Platforms and Very Large Online Search Engines on the mitigation of systemic risks for electoral processes pursuant to the Digital Services Act
https://ec.europa.eu/newsroom/repository/document/2024-13/C_2024_2121_1_EN_annexe_acte_autonome_cp_part1_v3_tpHHZgYyBGFMF8J5rE0OR1GdOis_103911.pdf, last accessed May 2024.

Farrand, B. (2024). Regulating misleading political advertising on online platforms: an example of regulatory mercantilism in digital policy. *Policy Studies*, 1–20. <https://doi.org/10.1080/01442872.2023.2258810>

Ferretti, M. P. (2016). Risk imposition and freedom. *Politics, Philosophy & Economics*, 15(3), 261-279. doi:10.1177/1470594X15605437

Galais, C., and A. S. Cardenal. 2017. “When David and Goliath Campaign Online: The Effects of Digital Media use During Electoral Campaigns on Vote for Small Parties.” *Journal of Information Technology & Politics* 14 (4): 372–386. <https://doi.org/10.1080/19331681.2017.1367347>.

Garnett, Holly Ann and Toby S. James (2020) Cyber Elections in the Digital Age: Threats and Opportunities of Technology for Electoral Integrity *Election Law Journal* 19(2): 1-16, DOI: 10.1089/elj.2020.0633

Gaultier-Gaillard, S., Louisot, JP.(2006) Risks to Reputation: A Global Approach. Geneva Pap Risk Insur Issues Pract 31, 425–445 (2006). <https://doi.org/10.1057/palgrave.gpp.2510090>

George C. (2019). Disinformation: A debate that needs to be better informed. Freedom from the Press. <https://blog.freedomfromthepress.info/2019/10/07/disinformation-2/>

Gibson, R., Bon, E., & Römmele, A. (2023). Operationalizing data-driven campaigning: designing a new tool for mapping and guiding regulatory intervention. *Policy Studies*, 1–17. <https://doi.org/10.1080/01442872.2023.2259333>

Gerbaudo, 2019. The digital party: Political organisation and online democracy. Pluto Press
Grohmann, R., & Corpus Ong, J. (2024). Disinformation-for-Hire as Everyday Digital Labor: Introduction to the Special Issue. *Social Media+Society*, 10(1). <https://doi.org/10.1177/20563051231224723>

Haenschen K. (2023). The conditional effects of microtargeted facebook advertisements on voter turnout. *Polit Behav.* 45(4): 1661–1681.

Jaurisch, J. 2020. “Rules for Fair Digital Campaigning.” Stiftung Neue Verantwortung e. V. Beisheim Center. Accessed August 1, 2022. https://www.stiftung-nv.de/sites/default/files/rules_for_fair_digital_campaigning.pdf.

Jones-Jang, S. M., Kim, D. H., & Kenski, K. (2021). Perceptions of mis- or disinformation exposure predict political cynicism: Evidence from a two-wave survey during the 2018 US midterm elections. *New Media & Society*, 23(10), 3105-3125. <https://doi.org/10.1177/1461444820943878>

Jungherr, A. (2016). Four Functions of Digital Tools in Election Campaigns: The German Case. *The International Journal of Press/Politics*, 21(3), 358-377. doi:10.1177/1940161216642597

Jungherr A., Schroeder R. (2023). Artificial intelligence and the public arena. *Communication Theory*, 33(3), qtad006. <https://doi.org/10.1093/ct/qtad006>

Kefford, G., Dommett, K., Baldwin-Philippi, J., Bannerman, S., Dobber, T., Kruschinski, S., Rzepecki, E. (2023). Data-driven campaigning and democratic disruption: Evidence from six advanced democracies. *Party Politics*, 29(3), 448-462. doi:10.1177/13540688221084039

Kim, Y. M., Hsu, J., Neiman, D., Kou, C., Bankston, L., Kim, S. Y., Raskutti, G. (2018). The Stealth Media? Groups and Targets behind Divisive Issue Campaigns on Facebook. *Political Communication*, 35(4), 515-541. doi:10.1080/10584609.2018.1476425

Klinke, A., & Renn, O. (2021). The Coming of Age of Risk Governance. *Risk Analysis*, 41(3), 407-557. doi:10.1111/risa.1338

Koc-Michalska, K., Klinger, U., Bennett, L., & Römmele, A. (2023). (Digital) Campaigning in Dissonant Public Spheres. *Political Communication*, 40(3), 255-262. doi:10.1080/10584609.2023.2173872

Kruck, A., & Weiss, M. (2023). The regulatory security state in Europe. *Journal of European Public Policy*, 30(7), 1205–1229. <https://doi.org/10.1080/13501763.2023.2172061>

Lavigne M. (2021). Strengthening ties: The influence of microtargeting on partisan attitudes and the vote. *Party Politics*, 27(5), 965–976. <https://doi.org/10.1177/1354068820918387>

Lupato, F. G., Jerez, A., & Meloni, M. (2023). Digital innovation in electoral campaigns: the case of microcredit in Podemos. *Policy Studies*, 1–19. <https://doi.org/10.1080/01442872.2023.2203479>

Matuszewski, P., & Szabó, G. (2023). The role of hyperactive Twitter accounts in the diffusion of political information. *Policy Studies*, 1–26. <https://doi.org/10.1080/01442872.2023.2237911>

Matthes, J., Hirsch, M., Stubenvoll, M., Binder, A., Kruikemeier, S., Lecheler, S., & Otto, L. (2022). Understanding the democratic role of perceived online political micro-targeting: longitudinal effects on trust in democracy and political interest. *Journal of Information Technology & Politics*, 19(4), 435–448. <https://doi.org/10.1080/19331681.2021.2016542>

Micova, Sally Broughton and Daniel Schnurr (2024) Systemic Risk in Digital Services: Benchmarks for Evaluating the Management of Risks to Electoral Processes – CERRE report, available at: <https://cerre.eu/publications/systemic-risk-in-digital-services-benchmarks-for-evaluating-the-management-of-risks-to-electoral-processes/>;

Mügge, D. (2023). The securitization of the EU's digital tech regulation. *Journal of European Public Policy*, 30(7), 1431–1446. <https://doi.org/10.1080/13501763.2023.2171090>

Novelli, Claudio and Formisano, Giuliano and Juneja, Prathm and Sandri, Giulia and Floridi, Luciano, Artificial Intelligence for the Internal Democracy of Political Parties (March 30,

2024). Centre for Digital Ethics (CEDE) Research Paper No. Forthcoming, Available at SSRN: <https://ssrn.com/abstract=4778813> or <http://dx.doi.org/10.2139/ssrn.4778813>

Rabinovich-Einy, Orna and Ethan Katsh, (2017) *Digital Justice Technology and the Internet of Disputes* Oxford: Oxford University Press

Ong J. C. (2020). Limits and luxuries of slow research in radical war: How should we represent perpetrators? *Digital War*, 1(1–3), 111–116. <https://doi.org/10.1057/s42984-020-00006-x>

Chicken, J. C., & Posner, T. (1998). *The Philosophy of Risk*. London: Thomas Telford Publishing.

Matthes, J., Hirsch, M., Stubenvoll, M., Binder, A., Kruikemeier, S., Lecheler, S., & Otto, L. (2022). Understanding the democratic role of perceived online political micro-targeting: longitudinal effects on trust in democracy and political interest. *Journal of Information Technology & Politics*, 19(4), 435–448. <https://doi.org/10.1080/19331681.2021.2016542>

Olson, Mancur (1971) *The Logic of Collective Action Public Goods and the Theory of Groups*. Harvard University Press.

Ringhand, L. A. 2021. "Foreign Election Interference: Comparative Approaches to a Global Challenge." *Election Law Journal: Rules, Politics, and Policy* 20 (1): 1–9. <https://doi.org/10.1089/elj.2020.0683>.

Sandri, G., Lupato, F. G., Meloni, M., von Nostitz, F., & Barberà, O. (2024). Mapping the digitalisation of European political parties. *Information, Communication & Society*, 1–22.

Simchon A, Edwards M, Lewandowsky S. (2024) The persuasive effects of political microtargeting in the age of generative artificial intelligence. *PNAS Nexus*. 3: 1-5. doi: 10.1093/pnasnexus/pgae035.

Schmidt, V. (2013) Democracy and Legitimacy in the European Union Revisited: Input, Output and 'Throughput' *Political Studies* 61(1): 2-22.

Schmidt, V. and M. Wood. (2019) "Conceptualizing Throughput Legitimacy: Procedural Mechanisms of Accountability, Transparency, Inclusiveness and Openness in EU Governance." *Public Administration* 97(4): 727-40.

Spitale, G. et al. (2023) AI model GPT-3 (dis)informs us better than humans. *Sci. Adv.* 9, DOI:[10.1126/sciadv.adh1850](https://doi.org/10.1126/sciadv.adh1850)

Time (2023) 'The Ultimate Election Year: All the Elections around the World in 2024', available at <https://time.com/6550920/world-elections-2024/>, last accessed May 2024.

Tenove, C., Buffie, J., McKay, S., & Moscrop, D. (2018). *Digital threats to democratic elections: How foreign actors use digital techniques to undermine democracy* [Report]. Centre for the Study of Democratic

Institutions. https://democracy2017.sites.olt.ubc.ca/files/2018/01/DigitalThreats_Report-FINAL.pdf

Waring. A., and Glendon. A. I., 1998. *Managing risk: critical issues for survival and success into the 21st century*. London: Thomson Learning.

Vliegenthart, R., Vrieling, J., Dommett, K., Gibson, R., Bon, E., Chu, X., de Vreese, C., Lecheler, S., Matthes, J., Minihold, S., Otto, L., Stubenvoll, M., & Kruikemeier, S. (2024). Citizens' Acceptance of Data-Driven Political Campaigning: A 25-Country Cross-National Vignette Study. *Social Science Computer Review*, 0(0). <https://doi.org/10.1177/08944393241249708>

Amy Vincent Sead Alihodžić Stephen Gale (2021) *Risk Management in Elections A Guide for Electoral Management Bodies*. Idea International and Australian Electoral Commission.

Tan, N. (2020). Electoral Management of Digital Campaigns and Disinformation in East and Southeast Asia. *Election Law Journal: Rules, Politics, and Policy*, 19(2), 1-26. doi:10.1089/elj.2019.0599

Vanden Eynde, G., & Maddens, B. (2021). Explaining digital campaign expenses: The case of the 2018 legislative elections in Colombia. *Journal of Information Technology & Politics*, 19(3), 302–315. <https://doi.org/10.1080/19331681.2021.1973643>

World Economic Forum (2024) *Global Risk Report 2024*, available at <https://www.weforum.org/publications/global-risks-report-2024/>; last accessed February 2024.

Ziegler, S. (2023). Watching the digital grassroots grow: assessing party members' social media campaigning during the 2021 German Bundestag election. *Policy Studies*, 1–21. <https://doi.org/10.1080/01442872.2023.2229248>

Zuiderveen Borgesius Frederik J., Judith Möller, Sanne Kruikemeier, Ronan Ó Fathaigh Kristina Irion, Tom Dobber, Balazs Bodo, Claes de Vreese (2018) *Online Political Microtargeting: Promises and Threats for Democracy*, *Utrecht Law Review*, pp. 82-96, DOI: [10.18352/ulr.420](https://doi.org/10.18352/ulr.420)