Bialystok Legal Studies
Białostockie Studia Prawnicze
2025 vol. 30 no. 4

sciendo

DOI: 10.15290/bsp.2025.30.04.14

Received: 01.04.2025
Accepted: 10.09.2025

Łukasz Augustyniak
Wrocław University of Science and Technology, Poland
lukasz.augustyniak@pwr.edu.pl
ORCID ID: 0000–0002–4090–4480

Michał Bernaczyk
University of Wrocław, Poland
michal.bernaczyk@uwr.edu.pl
ORCID ID: 0000–0001–7683–8852

Berenika Kaczmarek-Templin
Wrocław University of Science and Technology, Poland
berenika.kaczmarek@pwr.edu.pl
ORCID ID: 0000–0003–2731–7430

Unseen Influence: Computational Propaganda, Free Elections, and the Reluctance to Seek Judicial Remedies in Poland. Evidence from AI-Assisted Case Law Analysis

Abstract: The Polish electoral system adheres to the principle of free and fair elections. This principle has a defined content, and its backbone remains access to truthful information and the free shaping of opinions about a candidate or an issue put to a referendum. However, the enormous increase in computational power and the associated development of artificial intelligence have caused electoral competition to become highly aggressive; it no longer avoids false information, messages appealing to negative emotions, or calls for violence. Very Large Online Platforms' predictable abdication of their role as moderators of public debate leads to the question: How can or should public authorities protect integrity and freedom of participation from abuse in the era of digital constitutionalism? Should we rely on a litigation system where the initiative comes solely from the participant in the electoral process, or should we also include the regulatory power of the electoral administration? What picture of electoral campaigns is provided by Polish jurisprudence concerning electoral disputes?

Keywords: artificial intelligence, digital constitutionalism, Digital Services Act, Very Large Online Platforms, political advertisement, Digital Services Coordinator

Introduction

Discussion of the advantages and disadvantages of new technologies in the electoral process inevitably leads to the hotly debated issue of freedom of expression and the classic counterargument regarding the restriction of free speech through spending limits (both financial and material). This is particularly evident in the United States, which on the one hand has created the economic conditions for the development of information technologies and artificial intelligence, while on the other it has adopted First Amendment dogma followed by a restrictive approach to state or federal attempts to limit election campaigning (de Gregorio, 2022, p. 24; Urofsky, 2020, pp. 182–183 on McCutcheon v. Federal Election Commission, 572 US 185 (2014)). European constitutionalism is therefore faced with an interesting problem: political competition methods in EU countries are using tools from technological giants which have developed them without the legal restrictions typical of the European model of protecting freedom of speech or privacy. The European approach to the issue of free campaigning is thus a consequence of a belated conclusion that Very Large Online Platforms (VLOPs) and other digital market giants have built such a strong position that their relationship with the individual (user and potential voter) has begun to resemble the relations of power exercised by the state over an individual. At the same time, it should not be expected that with their increasing influence in the digital environment, large technological entities will take responsibility for the social, political, and economic effects of that influence. The enthusiasm at the end of the first decade of the 21st century that accompanied the inauguration of large platforms faded along with naive belief in self-regulation; this happened even before the reporting of another 'AI spring' in 2018 by the Artificial Intelligence Index (an initiative of Stanford University). Ironically, in 2019, Facebook's vice president of global affairs and communications, Nick Clegg, welcomed public regulations on content moderation with a slight rhetorical enthusiasm: 'Why should a private company decide who is or isn't a legitimate participant in an election?' (Sky News, 2019). This is a fundamental shift in narrative, considering that just a year earlier, Mark Zuckerberg had said, '[i]n a lot of ways Facebook is more like government than a traditional company' (Foer, 2017). Clegg, however, showed no courtesy towards European legislatures, but merely acknowledged the state of play in the European Union, as Member States had already begun to regain control over their citizens from online platforms.[1] Giovanni

1 A turning point is considered to be the Judgment of the Court of Justice of the European Union, 2014. The issues that supported the qualification of Google as a data controller (and not a data processor) – which can be easily nuanced in the areas of civil and administrative law as a technical-legal thread – fall under typically 'constitutional' arguments, rooted in the essence of public authority: 'The Court has already held that the provisions of Directive 95/46, in so far as they govern the processing of personal data liable to infringe fundamental freedoms, in particular the right to privacy, must necessarily be interpreted in the light of fundamental rights, which, accord-

de Gregorio (2022, pp. 20–24) has argued that the current shape of EU secondary law concerning digital services is a consequence of the 'reclaiming of state authority' by EU Member States through the European Union law oriented to the protection of human dignity. This began in the area of personal data protection with the adoption of the now obsolete Directive 95/46/EC, and accelerated with the entry into force of the Lisbon Treaty and the granting of binding status to the EU Charter of Fundamental Rights. Leading this trend were France, which experienced failed foreign interference in the 2017 French presidential elections ('#Macron Leaks'), and Germany, which adopted the 'Netzwerkdurchsetzungsgesetz' on 1 September 2017. The culmination of this process was the entry into force of the Digital Services Act (DSA), Regulation (EU) 2022/2065, which establishes rules for online platforms, content moderation, and intermediary liability, and applies to providers of digital services, including VLOPs.[2] The DSA affects electoral law primarily by imposing obligations on online platforms to combat disinformation, enhance transparency in political advertising, and mitigate risks to democratic processes. However, it should be noted that the effectiveness of the regulation will depend on the introduction at the national level of mechanisms for flagging and assessing illegal content, in accordance with electoral law. The DSA does not establish self-standing criteria for assessing what constitutes, for example, illegal or covert campaigning (Article 3(h)), nor does it impose general obligations to monitor the transmission or storage of information by providers of intermediary services. More importantly, it does not impose general obligations on such providers to seek facts or circumstances indicating illegal activity (Article 8). This means that the DSA should not be overestimated as a tool for protecting the integrity of the electoral system unless an effective system for safeguarding fair electoral competition is first established at the national level, adapted to mass, machine-driven, microtargeted political advertising, disinformation, or other harmful content that disrupts the electoral process.

The issue is significant for Poland, as in the area of electoral law, it denied this regulatory trend through an amendment to the Electoral Code in 2018 (Sejm of Poland, 2018), despite the risk of foreign interference (Bernaczyk, 2020, pp.).[3] From the perspective of 2025, it can be concluded that the 2018 amendments were done for short-term political goals (to conceal the transfer of public funds to the campaigns of the then ruling right-wing majority), but third-party campaign deregulation, for example, came at the cost of increased national security threats (allowing agitation

ing to settled case-law, form an integral part of the general principles of law whose observance the Court ensures and which are now set out in the Charter' (§68).

2 The Digital Services Act (DSA) entered into force on 1 November 2022. However, the full application of its provisions began on 17 February 2024, due to a transitional period for platforms to adapt to the new requirements.

3 The legal framework of campaigning is shaped primarily by Section I Chapter 12 Section IX of the Electoral Code of 2011 (Sejm of Poland, 2011).

funded by unknown sources and origins). The Polish Electoral Code of 2011 did not recognize the peculiarities of electoral campaigning on the internet, nor did it foresee the development of large platforms or campaigning supported by algorithms. This is surprising, because constitutional standards do not allow for the assumption that competition in an election campaign should be based on the exercise of freedom of expression entirely free from intervention by public authorities. In 2009, a judgment by the Polish Constitutional Tribunal (2008, section III(3) of the legal reasoning) ruled that the rule-of-law clause implies the state's positive obligation to create conditions conducive to the fair and safe exercise of freedom of political expression:

> Article 2 of the Constitution implies, among other things, the legislature's duty to establish regulations that ensure a fair electoral campaign, allowing citizens access to truthful information about public affairs and candidates. The electoral campaign should facilitate the free formation of the voter's will and the making of decisions expressed through the act of voting.

This view was not new, as the Court had already outlined the essential components of free elections in 2008, including (i) 'genuine freedom of expression and assembly', (ii) 'the overall media order in the state', (iii) accessibility to the local media market, (iv) transparent procedures for obtaining the necessary financial resources for campaigning, and (v) adequate and effective guarantees for the protection of electoral rights (Judgment of the Polish Constitutional Tribunal, 2006). A distinctive feature of this reasoning is the connection between freedom of expression and the fundamental principles of the political system. There is a resemblance to the reasoning in the Romanian Constitutional Court's judgment no. 32 of 6 December 2024, on the annulment of the electoral process for the election of the president of Romania that year.[4] The Romanian court ordered the entire electoral process be repeated, deriving this conclusion primarily from the principle of national sovereignty (Article 2 of the Constitution of Romania), making Romania the first country in Europe to respond so decisively to computational propaganda deployed in national elections.[5]

Polish electoral law remains at the stage of diagnosis established relatively early in 2018, rather than of the implementation of practical solutions. The Polish National Electoral Committee (Państwowa Komisja Wyborcza) (NEC) voiced concerns regarding the electoral system on 26 September 2018, by publishing a document en-

4 In the reasons for its judgment, the Court stated that the electoral process for the presidential election in 2024 fell victim to 'the manipulation of electors' votes and the distortion of the equality of opportunity for the electoral competitors, through the non-transparent use of digital technologies and artificial intelligence in the electoral campaign, in violation of electoral legislation, and through funding from unreported sources in the electoral campaign, including the online one' (§11).

5 Samuel C. Woolley and Philip N. Howard (2016) define computational propaganda as the combination of social media platforms, independent intermediaries, algorithms, and big data technology implemented to manipulate public opinion.

titled 'The National Electoral Committee's position on the principles of conducting and financing an electoral campaign on the internet' (Państwowa Komisja Wyborcza, 2018). The NEC's communication completely departed from broadcasts on radio and television, and for the first time in Polish history, focused exclusively on the topic of electoral agitation conducted on the internet, placing the manner in which it is carried out in a rather pejorative context.[6] This allegation fell on deaf ears, which was easy to explain on a political level. The United Right (Zjednoczona Prawica, the political alliance in power from the 2015 elections until its defeat in 2023) showed no willingness to strengthen the transparency of electoral campaigns nor to adapt them to modern requirements. This does not change the constitutional paradigm, in which the Electoral Code must provide effective legal remedies against 'electoral materials, particularly posters, leaflets, and slogans, as well as statements or other forms of electoral propaganda containing false information' (Article 111 §1 of the Electoral Code).

This article aims to examine the image of electoral campaigns based on disputes conducted under Article 111 of the Electoral Code. The latter introduced a specific expedited procedure for claims in Polish law, somewhat resembling the protection against violations of personal rights but granted exclusively to candidates or authorized representatives of an interested electoral committee. We are interested in the scale of applications filed against various forms of digital campaigning, based on the reasoning of court rulings published in the Portal of Common Courts' Decisions. We believe that examining over 400,000 disclosed cases will help to answer the question of how many disputes related to digital election campaigning actually reach the courts. The use of an AI model allowed us to determine, first, what plaintiffs challenge in court as false election campaigning; second, how much digital content is contested in this manner; and finally, what the number of such cases tells us about the tendency of voters and political actors to compete in a legal way. A working hypothesis assumed that the Polish ecosystem of social and 'traditional' media (radio and linear television) has created two separate worlds, one in which election disputes are addressed by individuals and committees in courts of law, and one where there is an all-out war on social media, where the sheer speed and scale of blows exchanged between opponents make correcting misinformation through electoral procedures futile (the need for a symmetrical response outweighs the truth and accountability expected from a court's decision). We will first examine the key foundations of litigation in election-related cases; we will then provide the results of a machine-based

6 The NEC explicitly described the practice of 'political parties, election committees, candidates, and other entities participating in public life' as conducted by 'means commonly considered unethical and sometimes illegal'. The communication gives several examples of 'all kinds of messages' classified as electoral material, e.g. on websites used by electoral committees to conduct electoral agitation, but also disseminated in another form, including in the form of messages 'multiplied by persons or by automated systems on behalf of a committee' (Państwowa Komisja Wyborcza, 2018, p. 2).

analysis of Polish case law related to these matters. In the subsequent section, we will attempt to explain how the pseudo-anonymity of the digital environment may discourage the resolution of such cases in courts of law and what alternatives may be provided in the foreseeable future under national and EU law.

1. Legal proceedings against the dissemination of false information in electoral campaigns

The freedom to express opinions is linked to responsibility for both the opinions themselves and the manner in which they are expressed. Legal provisions must create the necessary conditions for this, in the interests both of those who wish to exercise their freedom of expression and of those who may be affected by it due to its content or form. Article 111 of the Electoral Code provides candidates or the official representative of an electoral committee with the ability to combat false information in electoral materials. The legal protection measures specified in Article 111, although undoubtedly the fastest, do not constitute the only legal avenue for candidates to assert their rights in court. Other available legal remedies include the right of rectification, regulated by Articles 31a–33 and 39 of the Press Law Act, as well as lawsuits for the protection of personal rights under Articles 23–24 and 448 of the Civil Code. All these proceedings are conducted under the provisions of the Code of Civil Procedure.

Court cases initiated under Article 111 of the Electoral Code are civil cases in a formal sense (Article 1 of the Code of Civil Procedure). Under the Electoral Code, their examination is subject to the provisions of the Code of Civil Procedure governing non-contentious proceedings, which means that the regulations set out in Articles 506–525 of the Code of Civil Procedure apply. However, the Electoral Code modifies the general rules, particularly concerning the timeframe of the proceedings. According to Article 111 §§2–3 of the Electoral Code, a district court examines the application within 24 hours. A district court decision may be appealed to a court of appeal within 24 hours, and the court of appeal must resolve the appeal within the same timeframe. No cassation appeal is allowed against the decision of the court of appeal, and the decision is subject to immediate enforcement. This means that from the moment of filing the application to the execution of the decision, no more than 72 hours should pass.

The extremely short timeframes for handling cases in the first and second instance aim to ensure that, on the one hand, voters can familiarize themselves with the court's findings before election day, and on the other, that the pre-election debate remains fair and free from false information (Judgment of the Constitutional Tribunal, 2008). Expedited proceedings in electoral matters come with a trade-off: a narrow list of plaintiffs (limited to a 'candidate or the election representative of the concerned electoral committee') may seek remedies for infringements not caused by the proliferation of 'any information' but only by such information that constitutes 'electoral materials, in particular posters, leaflets, and slogans, as well as statements or other

forms of electoral campaigning'. Unlike the general term 'information', a claim may concern only three types of harmful objects: electoral materials, statements, or other forms of electoral campaigning (Article 111 §2 of the Electoral Code).

'Electoral material' is not an open-ended legal term, nor is 'electioneering': both of these phrases have been defined in the Electoral Code. Electoral material is any publicly disseminated and recorded message originating from an electoral committee that is related to the announced elections (Article 109 §1 of the Electoral Code). Electioneering is the public encouragement to vote in a particular way, especially for a candidate of a specific electoral committee. Thus 'other forms of electoral campaigning' may cover third-party campaigning conducted without the consent of electoral committees, regardless of its domestic or foreign origin. This controversial issue has been raised in Poland since 2020 by the Organization for Security and Co-operation in Europe (ODIHR, 2020, p. 3), as third parties are not required to label their physical or digital forms of campaigning, which makes them difficult to identify for the purpose of expedited proceedings in electoral matters.

Another issue concerns the very concept of electioneering, which requires public encouragement, raising problems in the case of microtargeting. Microtargeting can be so sophisticated that electioneering loses the characteristics of a mass, identical ('public') message, making it difficult to classify as action falling under the traditional rules on electioneering. Last but not least, electioneering does not have to target a candidate personally, nor their electoral programme; instead, it can, for example, discourage people from voting, thereby manipulating voter turnout. This in turn can be concealed within forms of expression that blend into the general entertainment content of social media platforms, such as fostering a general aversion to the state, promoting the boycott of any civic engagement, or instilling in the audience the feeling that their civic participation is meaningless. Due to the cost of and barriers to accessing private telecommunications data, it is doubtful that electoral committees would be able to monitor the scale of such information operations.

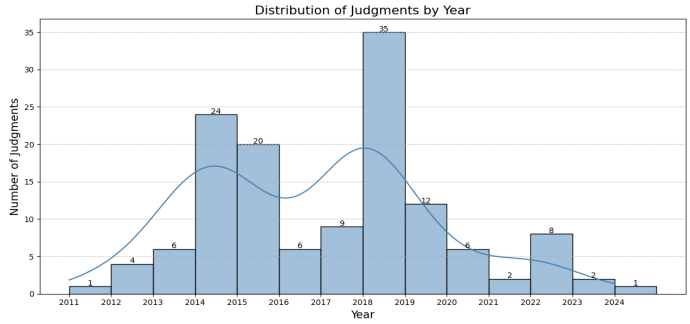
2. What does the courts' practice tell us about the nature of election-related disputes?

From the technological perspective, our examination of case law was conducted using state-of-the-art Natural Language Processing techniques and Human-In-The-Loop open-source software, developed within the JuDDGES: Judicial Decision Data Gathering, Encoding, and Sharing project.[7] The team examined Article 111 disputes re-

7 The work was partially supported by the JuDDGES project (Judicial Decision Data Gathering, Encoding and Sharing), funded by the National Science Centre (NCN), Poland, under the CHIST-ERA programme (project number 2022/04/Y/ST6/00183). Additional support was provided by the Department of Artificial Intelligence at Wroclaw University of Science and Technology.

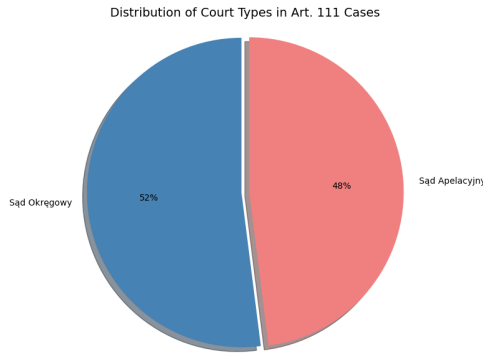
garding online campaign materials by querying over 2 million judicial decisions. After refining our search, we found 136 cases related to digital electioneering. A histogram (Figure 1) revealed the sparse number of cases, with clusters in 2014 and 2018 coinciding with local elections. Moreover, in 2015, following a few elections, we observed that the rulings within the judicial system were still for the 2014 local elections. Only two cases have been related to presidential elections. In conclusion, despite millions of rulings published and available in our internal search database, only a little more than 100 judgments have covered this topic in the past decade. This could mean that our estimates of the impact of third-party campaigning on elections might be less accurate than expected; while everyone discusses it, few take the step to file a case.

Figure 1. Number of judgments, 2011–2025.



Our research team found that judgments related to digital electioneering disputes were distributed across various courts, with 52% of the decisions coming from district courts (Sąd Okręgowy) and 48% from appellate courts (Sąd Apelacyjny) (see Figure 2). These findings underscore the involvement of various judicial levels in addressing the challenges presented by online campaign materials.

Figure 2. Type of court.



3. The problem of identifying wrongdoers on the internet

One of the most essential requirements is the identification of the parties, including their names or legal entities, and their legal representatives and attorneys, as well as their addresses (Piesiewicz & Piaskowska, 2018). Since a court is not authorized to proceed with a case without this information, an applicant seeking claims under Article 111 of the Electoral Code must identify the person engaged in an action that constitutes a violation and must demonstrate that this person engaged in the alleged conduct. The legislature has not modified the rules when the contested action in the application occurred on the internet, a VLOP, etc. Therefore the applicant must designate the participant at the stage of submitting the application, specify the unlawful action attributed to them, and subsequently prove the truthfulness of their claims before the court. The verification of the applicant's claims does not involve actions aimed at determining the identity of individuals who posted false or unlawful information on the internet, but rather whether the alleged perpetrator is indeed the one involved, as the request in the application pertains to them.

In cases of online violations, a candidate (or the electoral committee's representative) may face difficulties in determining the identity of the individual responsible, especially within the timeframe required for this specific procedure. The ECHR's position in *Staniszewski v. Poland* increases the burden put on the applicant: while the swift resolution of election-related disputes may be desirable, it should not lead to an excessive limitation of procedural guarantees granted to the parties to such proceedings, particularly the defendants.

A candidate (or an election committee representative) seeking protection for his/her rights which have been violated on the internet must apply the general rules of civil procedure. These require an entity to be identified by first name and surname (Kaczmarek-Templin, 2014); furthermore, the law imposes an obligation on the party initiating the proceedings to provide the defendant's place of residence or registered office and address (Articles 126 §1 and 187 §1, in conjunction with Article 13 §2 of the Code of Civil Procedure). The absence of this information in the application will result in the return of the statement of claim (Article 130 of the Code of Civil Procedure). Information on who specifically can be held responsible for disseminating false information during an election campaign should be obtained before the proceedings are initiated.

The Supreme Court of Poland's judgment of 6 August 2020, addressed cases involving the violation of personal rights, but the issue analysed was a more universal problem related to the identification of the party violating the rights of an injured party on the internet, which is worth examining in more detail. The Court took the position that obtaining information about the perpetrator's identity can be based on

the rules on the seizure of evidence (Articles 310 of the Civil Procedure Code).[8] In the Court's view, these provisions should allow the contact details of the potential infringer to be secured, if those details are known to a third party. This view seems to contradict the general rules related to civil procedure, namely the principle that the court cannot assist a party in actions related to determining the procedural legitimacy of the parties. The provisions on securing evidence concern assistance in determining specific circumstances from which a party derives legal consequences, rather than providing a basis for identifying the entity that should be a party in the case. Identifying the party cannot be qualified as evidence in the proceedings. Therefore the court's stance may seem to be an expression of activism, in light of the lack of legislative response to conflicts in the digital environment.

4. Blind lawsuits and forgotten expeditious examinations of election-related disputes

For years, the challenge of identifying entities acting online has been a topic of legal debate (Pązik, 2022; Wybrańczyk, 2023), leading to the emergence of the so-called 'blind lawsuit' concept, which aims to enable victims to pursue legal claims for personal rights violations even when the wrongdoer's identity cannot be determined. The first attempt to translate the concept into law came in 2017, when a draft parliamentary bill amending the Civil Procedure Code and the Telecommunications Law was submitted, but which was rejected at first reading. This draft proposed allowing the filing of a lawsuit for the violation of personal rights against a person unidentified by name, with the burden of identifying the defendant placed on the court (Sejm of Poland, 2017).

In 2024, with the submission of another parliamentary bill amending the Civil Procedure Code, the idea of the so-called 'blind lawsuit' targeted at an unknown person resurfaced (Sejm of Poland, 2024). This bill introduces a separate procedure in cases of the protection of personal rights against individuals of unknown identity. Although the draft moved away from the anachronistic (and narrow) language of the 2017 proposal, which referred to 'violations on the internet', in favour of a broader concept of 'violations through means of electronic communication', the issue for participants in electoral campaigns remains the exclusivity of this procedure. According to the proposed Article 505 §40 of the Civil Procedure Code, the provisions would apply to cases concerning the protection of personal rights if the violation occurred electronically and the plaintiff does not know the first name, surname, or address or registered office of the defendant who violated their personal rights. Upon the plaintiff's request, the court will

8 According to this regulation, even before the initiation of proceedings, the court may, at the request of the interested party, secure evidence if there is a concern that its collection will become impossible or excessively difficult, or when there is a need to confirm the existing state of affairs for other reasons.

oblige the service provider through whom the violation of personal rights occurred to send all the data it holds about the defendant, under the penalty of a fine (proposed Article 505 §42(1) of the Civil Procedure Code). However, as indicated by the aforementioned provisions, the methods of determining the identity of the violator will apply only to proceedings concerning violations of personal rights and, by analogy, cannot be applied to proceedings initiated under Article 111 of the Electoral Code, despite their similar nature. This means that even if the provisions in the so-called 'blind lawsuit' are enacted, they will be completely useless in expeditious electoral procedures. In the case of the spread of false information in electoral materials on the internet, the only way to eliminate it will be a case for the violation of personal rights, which will not have the characteristics of an expedited procedure as defined in the provisions concerning electoral campaigns. Under the general rules of procedure, it would take years for the court to issue a verdict, which contradicts the fairness of the electoral process. Given, for example, the mass automated mechanism of attacks during a campaign, an applicant would be unable to respond quickly and fight directly with the unknown violator or, more importantly, to present to the intermediary digital platforms a judgment obtained through an expeditious procedure.

Although the electoral procedure cannot be applied, the proposed amendment should be viewed positively, as the injured party will ultimately be able to pursue their rights through legal action. However, the legislative process is still pending, so we cannot yet determine whether the issue of fair electoral competition will be ignored.

Conclusions

In a situation where election materials containing false information are disseminated on the internet, the right to a court trial based on Article 111 of the Electoral Code is essentially illusory. In such a case, the possibility of initiating legal proceedings arises only from the formal right to a court (Florczak-Wątor, 2016). However, the possibility of effectively obtaining legal protection remains questionable; in fact, one could consider whether this constitutes a violation of the constitutional right to a court (Zalewski & Zdanowicz, 2025). While a rights-holder may pursue claims for the infringement of personal rights, even a favourable verdict would be futile, as it would inevitably come post-election. The analysis of case law available in the Case Law Portal supports this conclusion. The number of judgments issued under Article 111 is relatively small, and observation of internet users' activity in the pre-election period suggests that there are significantly more violations which never reach court. Thus the quantitative analysis of election disputes recorded in the official repository confirms the validity of our hypothesis that an anachronistic law, tailored to campaigns in the bygone era of analogue media (radio, linear television, physical billboards in the public space), has created two separate worlds: one in which election

disputes are addressed by individuals and committees in a court of law, and the other as all-out war on social media platforms, where no one intends to resolve conflicts in a civilized manner but rather seeks to overwhelm the opponent with aggressive and abusive messaging. The Polish framework, which fails to align with the digital environment of voter activity, cannot be reduced to a matter of mere political discretion, for electoral law that does not provide sufficient safeguards for the fairness of the electoral process falls short of a constitutional imperative.

However, there is light at the end of the tunnel, if we take into consideration the entry into force on 10 October 2025 of Regulation (EU) 2024/900 of the European Parliament and of the Council of 13 March 2024 on the Transparency and Targeting of Political Advertising. Publishers of political advertising will be under an obligation to label political advertisements, including (but not limited to) transparency regarding the use of microtargeting and AI systems, and to maintain records documenting the financial trail from sponsors to the final communication (see Articles 9–12 of Regulation 2024/900).[9] It should be added that political advertising disseminated by VLOPs is already subject to the transparency obligation laid down in Article 39 DSA (Jabłonowska, 2024). No less important – and indeed of primary relevance in the context of this paper – is the horizontal right of access to information (Article 17 of Regulation 2024/900) concerning political advertising granted to interested entities (vetted researchers, members of civil society organizations, political actors, national and international election observers, and journalists). Regulation 2024/900 may enhance the chances of identifying the defendant in an electoral dispute, and on top of that, it attempts to address the problem we have described concerning hostile actors, whereas these actors, by default, pursue ways to outmanoeuvre legal constraints and to blend into the political campaign ecosystem. While the Regulation adopts a solution similar to that of the Polish Electoral Code, namely by excluding from its scope political expressions made in a 'personal capacity' (Article 2 §2 of Regulation 2024/900, similar to third-party campaigning in Poland conducted outside the structures of an electoral committee), it nevertheless establishes a mechanism for detecting, inter alia, political advertisements which are suspected of concealing a professional, paid information operation disguised as grassroots campaigning (Chapters 22 and 23 of Regulation 2024/900).

Another element in safeguarding the integrity of the electoral system may be the notice-and-action mechanism provided for in Article 16 DSA. It must be stressed, however, that Regulation (EU) 2022/2065 does not contain provisions empowering platforms or public authorities to remove or block political advertising, as defined under national electoral law. Nevertheless, it does establish rules enabling the removal or dis-

9 Publishers of political advertising are defined as providers of political advertising services, usually at the end of the chain of service providers, who publish, deliver, or disseminate political advertising by broadcasting, making it available through an interface, or otherwise making it available to the public.

abling of access to such content, which in specific circumstances may overlap with the notion of electoral campaigning under Polish law or may produce equivalent campaign effects (for instance, the dissemination of the stolen internal correspondence of electoral committees, as in the Macron Leaks incident, or the 2021 hack-and-leak scandal involving the disclosure of 60,000 emails from the head of the Polish prime minister's office, Michał Dworczyk). In practice, the procedure under Article 16 DSA will be most effective where the applicant can demonstrate the unlawfulness of the content on the basis of a judicial determination rendered in expedited electoral proceedings. However, the latter is not required by the DSA, and the classification of information as illegal (including false information) may result from an autonomous legal assessment of the entity hosting the disputed information or activity (Article 16 §4 DSA).

Failure to comply with the DSA's notice-and-action procedure may result in a complaint to the president of the Office of Electronic Communications (Prezes Urzędu Komunikacji Elektronicznej), who serves in Poland as the Digital Services Coordinator. This means that this president should enjoy guarantees of independence similar to those of the supervisory authority under the GDPR, albeit less firmly anchored in EU law, since the independence of data protection supervisory authorities is based directly on the EU Charter of Fundamental Rights. National coordinators must nevertheless be granted a comparable status under domestic law by means of so-called guarantees of functional independence, which should shield them from political pressure through the manner of their appointment, fixed terms of office, and protection against removal (Łakomiec, 2024). This also gives rise to an interesting constellation in Polish constitutional law, insofar as the competence envisaged for the president of the Office of Electronic Communications to exercise authoritative powers against unlawful digital content of a political nature and/or which qualifies as electoral campaigning shall entail his/her inclusion within the broadly conceived category of the electoral administration system (Gąsior, 2015). Similarly, albeit on a narrower scale, the institutional position of the president of the Personal Data Protection Office within the constitutional framework may be assessed, as this authority is empowered to intervene in cases of the unlawful processing of personal data – for example, the public disclosure of personal data by candidates in the course of electoral campaigning, as indeed occurred during the rivalry between Nawrocki and Trzaskowski in the 2025 presidential election campaign. It should be borne in mind, however, that these are instruments of public supervision and ought to complement, rather than replace, an effective system of judicial protection through expedited electoral litigation. Nevertheless, the anachronistic character of Polish electoral law may, over time, awaken political actors' interest in the administrative powers of the president of the Office of Electronic Communications. Our analysis has confirmed that the system of judicial protection attracts only negligible interest in the context of digital campaigns – and it is these campaigns that will constitute the future of political marketing.

The absence of statutory provisions in Polish electoral law that specifically address digital election campaigning also reveals an interesting paradox: while the European Union is under constant pressure and criticism as a supranational institution that allegedly restricts the sovereignty of its Member States, it is in fact the Union that adopts measures aimed at safeguarding the integrity of the democratic electoral process against covert intervention by foreign actors and sponsors – interventions that strike at the very principle of a Member State's national sovereignty.

REFERENCES

Bernaczyk, M. (2020). Polski kodeks wyborczy wobec manipulacji i innych form propagandy obliczeniowej. In M. Bernaczyk, T. Gąsior, J. Misiuna, & M. Serowaniec (Eds.), *Znaczenie nowych technologii dla jakości systemu politycznego: ujęcie politologiczne, prawne i socjologiczne* (pp. 83–87). Uniwersytet Mikołaja Kopernika w Toruniu Wydawnictwo Naukowe.

de Gregorio, G. (2022). *Digital constitutionalism in Europe: Reframing rights and powers in the algorithmic society*. Cambridge University Press.

European Parliament and European Council. (1995, 24 October.) Directive 95/46/EC on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data (O. J. L 281, 23.11.1995).

European Parliament and European Council. (2022, 19 October) Regulation (EU) 2022/2065 on a Single Market for Digital Services and Amending Directive 2000/31/EC (Digital Services Act) (O. J. L 277).

European Parliament and European Council. (2024, 13 March). Regulation (EU) 2024/900 on the Transparency and Targeting of Political Advertising (O. J. L 2024/900, 20.03.2024).

European Union. (2000). Charter of Fundamental Rights of the European Union of 7 December 2000 (O. J. C 202, 2016).

European Union. (2007, 13 December). The Treaty of Lisbon amending the Treaty on European Union and the Treaty Establishing the European Community of 13 December 2007 (O. J. C 306).

Florczak-Wątor, M. (2016). Prawo do sądu jako prawo jednostki i jako gwarancja horyzontalnego działania praw i wolności. *Przegląd Prawa Konstytucyjnego*, *3*, 47–66.

Foer, F. (2017, 19 September), Facebook's war on free will. *The Guardian*. https://www.theguardian.com/technology/2017/sep/19/facebooks-war-on-free-will

Gąsior, T. (2015). *Kontrola finansowania komitetów Wyborczych. Zagadnienia administracyjnoprawne*, Wydawnictwo Sejmowe, Warszawa, 2015.

Jabłonowska, A. (2024). Commentary on Article 39 of the Digital Services Act (Regulation (EU) 2022/2065 of the European Parliament and of the Council. In M. Grochowski (Ed.), *Rynek Cyfrowy. Komentarz* (pp. 358–363). Wydawnictwo C.H. Beck, Warszawa.

Judgment of the Court of Justice of the European Union of 13 May 2014 on the case of *Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos (AEPD), M. C. González*, C 131/12.

Judgment of the European Court of Human Rights of 14 October 2021 on the case of *Staniszewski v. Poland*, application no. 20422/15.

Judgment of the Polish Constitutional Tribunal of 3 November 2006, K 31/06, OTK-A 2006, no. 10, item 1.

Judgment of the Polish Constitutional Tribunal of 21 July 2008, K 7/09, OTK-A 2009, no. 7, item 113.

Judgment of the Polish Supreme Court of 6 August 2020, case no. III CZP 78/19. https://www.sn.pl/sites/orzecznictwo/OrzeczeniaHTML/iii%20czp%2078–19.docx.html

Judgment of the Romanian Constitutional Court of 6 December 2024, no. 32.

Kaczmarek-Templin, B. (2014). Odpowiedzialność administratora portalu. In M. Małek, K. Serafin, & E. Mazurek (Eds.), *Etyka i technika. Społeczne i etyczne aspekty działalności inżynierskiej* (pp. 119–126). Studium Nauk Humanistycznych i Społecznych Politechniki Wrocławskiej, Wrocław.

Łakomiec, K. (2024). Commentary on Article 50 of the Digital Services Act (Regulation (EU) 2022/2065 of the European Parliament and of the Council. In M. Grochowski (Ed.), *Rynek Cyfrowy. Komentarz* (pp. 421–424). Wydawnictwo C.H. Beck, Warszawa.

Office for Democratic Institutions and Human Rights. (2020, 23 September). *Republic of Poland: Presidential election, 28 June and 12 July 2020. ODIHR Special election assessment mission final report*. https://www.osce.org/files/f/documents/6/2/464601.pdf

Państwowa Komisja Wyborcza. (2018). National Electoral Committee's position on the rules for conducting and financing an electoral campaign on the internet of 26 September 2018 (ZKF-811–850/18), op. https://pkw.gov.pl/uploaded_files/1537988216_1–50-18.pdf

Pązik, A. (2022). Ślepy pozew i krótkowzroczny ustawodawca': uwagi na marginesie projektu ustawy o wolności słowa w Internecie. In B. Fischer, A. Pązik, & M. Świerczyński (Eds.), *Prawo sztucznej inteligencji i nowych technologii* (pp. 367–397). Wolters Kluwer.

Piesiewicz, P., & Piaskowska, O. (2020). Ustalenie danych osobowych sprawcy naruszenia dóbr osobistych w Internecie celem dochodzenia ich ochrony w postępowaniu cywilnym. *Zeszyty Naukowe Katolickiego Uniwersytetu Lubelskiego Jana Pawła II*, *61*(2), 277–289. https://doi.org/10.31743/zn.2018.61.2.277–289.

Sejm of Poland. (2018). Act of 11 January 2018 Amending Certain Acts in Order to Increase Citizens' Participation in the Process of Election, Functioning and Control of Certain Public Bodies (Journal of Laws of 2018, item 130).

Sejm of Poland. (2024). Parliamentary Bill no. 728 Amending the Code of Civil Procedure Act and Certain Other Laws.

Sky News. (2019, 25 June), *Sir Nick Clegg: Facebook welcomes government regulation*. https://news.sky.com/story/sir-nick-clegg-link-between-social-media-and-mental-health-problems-not-proven-11748174

Urofsky, M. I. (2020). *The campaign finance cases:* Buckley*,* McConnell*,* Citizens United *and* McCutcheon. University Press of Kansas.

Woolley, S. C., & Howard, P. N. (2016). Political communication, computational propaganda, and autonomous agents. *International Journal of Communication*, *10*, 4886.

Wybrańczyk, D. (2023). Propozycja wprowadzenia do procedury cywilnej tzw. ślepych pozwów. *Zeszyty Prawnicze Biura Analiz Sejmowych Kancelarii Sejmu*, *1*, 159–173.

Zalewski, M., & Zdanowicz, U. (2025). Realność ochrony dóbr osobistych naruszonych za pośrednictwem internetu a konstytucyjna gwarancja prawa do sądu. *Palestra*, *1*, 176–191.