Bialystok Legal Studies
Białostockie Studia Prawnicze
2026 vol. 31 no. 1

sciendo

DOI: 10.15290/bsp.2026.31.01.01

Received: 05.12.2025
Accepted: 15.03.2026

Artur Olechno
University of Bialystok, Poland
a.olechno@uwb.edu.pl
ORCID ID: 0000–0003–2594–0376

Sabina Grabowska
University of Rzeszów, Poland
sgrabowska@ur.edu.pl
ORCID ID: 0000–0003–0530–708X

Hubert Kotarski
University of Rzeszów, Poland
hkotarski@ur.edu.pl
ORCID ID: 0000–0002–5370–7099

Towards a Digital Rule of Law: Redefining Citize –State Relations in Digital-Age Democracies[1]

Abstract: This article examines the normative tensions between classical conceptions of the rule of law and the structural transformation of democratic governance in the digital age. The main research hypothesis is that classical rule-of-law frameworks are no longer sufficient in the face of algorithmic opacity, the power of platforms, and automated decision-making, which necessitates the development of a renewed concept of a digital rule of law. The study employs three complementary methods: the dogmatic-legal method (analysis of EU legal acts, in particular the Digital Services Act, the AI Act, and the GDPR), the theoretical-legal method (analysis of the concept of the rule of law), and critical discourse analysis in relation to digital transformation. It argues that digitalisation is not merely a technical shift but a reconfiguration of the citizen–state relationship. On this basis, it develops three normative directions: digital

1 Funded by the National Science Centre, Poland, under the OPUS call in the Weave programme (UMO-2023/51/I/HS5/01417), and the Flemish Research Foundation (FWO Funding Agreement G000325N). The article is also financially supported by the Polish Minister of Science under the 'Regional Initiative of Excellence' (RID) programme.

constitutionalism as a framework for legitimising digital infrastructures, legal safeguards for public and platform-based uses of artificial intelligence, and more inclusive models of civic participation in digitally mediated lawmaking. The article concludes by formulating institutional recommendations for operationalising a digital rule of law in contemporary democracies.

Keywords: digital democracy, rule of law, digital constitutionalism, civic participation, artificial intelligence, AI regulation, algorithmic governance

Introduction

Contemporary democracy is undergoing a profound transformation that is not only technological but also structural and normative. This article assumes that the digitisation of democratic processes signifies more than a mere technological enhancement or a shift in the medium of information. Rather, it constitutes a fundamental transformation in the structure of citizen–state relations, leading to a shift from equality before the law to profiling, from transparent procedures to algorithmic decision-making, and from deliberation to microtargeting (Caruso, 2025). This tension is especially evident in the context of recent European Union regulations, namely the Digital Services Act (DSA) and the AI Act, which are particularly relevant because they seek to regulate the power of platforms, algorithmic governance, and the use of artificial intelligence in ways that directly affect democratic processes and fundamental rights (Pane, 2025).

The aim of this article is to determine whether, and to what extent, algorithmic governance and platform-based public communication can be reconciled with the principles of procedural justice, transparency, accountability, and individual autonomy, and whether this requires the reformulation of the classical concept of the rule of law into a model of a digital rule of law. The main research hypothesis is that the classical frameworks of the rule of law are insufficient in the face of algorithmic opacity and platform-based governance, which necessitates the development of a new concept of a digital rule of law. This concept should preserve the core elements of legality, transparency, accountability, and procedural fairness, while adapting them to the conditions of a platformised public sphere and automated decision-making. Two auxiliary hypotheses follow from this assumption. First, Habermas' conception of the public sphere remains a useful normative point of reference for assessing the quality of deliberation under digital conditions. Second, current EU regulatory instruments such as the DSA and the AI Act, although significant, do not fully resolve the structural tension between the logic of law and the logic of algorithms.

To verify these hypotheses, we employ three complementary research methods: the dogmatic-legal method, consisting of the analysis of EU legal acts, in particular the DSA and the AI Act; the theoretical-legal method, focused on the concept of the rule of law and its possible reformulation under digital conditions; and critical discourse analysis, used to examine how digital transformation reshapes the language

and normative assumptions of democracy, governance, and public communication. The article is structured as follows: the first part reconstructs classical concepts of the rule of law and the main models of digital democracy. The second part discusses the transformation of public institutions and citizen–state relations in the digital age. The third and fourth parts analyse the democratic opportunities and risks associated with digital technologies, while the final part formulates normative proposals for operationalising a digital rule of law.

1. Classical approaches to the rule of law and models of digital democracy

The rule of law is one of the constitutive principles of western constitutional democracy. In the context of digital transformation, however, it can no longer be understood solely as a classical guarantee against arbitrary state power. Today, the conditions under which power is exercised are increasingly shaped by platforms, data infrastructures, and algorithmic systems. For this reason, revisiting classical theories of the rule of law is not purely a historical exercise; it is necessary in order to determine whether the emerging digital order can still meet the minimum standards of legality, accountability, transparency, and procedural justice.

This is why the present article returns to A. V. Dicey, Lon L. Fuller, and John Rawls; their concepts provide three complementary perspectives that are directly relevant to the idea of a digital rule of law. Dicey draws attention to the problem of arbitrary power and the requirement that authority remain subject to law. Fuller offers criteria for assessing whether governance remains intelligible, predictable, and procedurally coherent. Rawls, in turn, makes it possible to ask whether institutional arrangements remain fair from the standpoint of equal citizenship. Taken together, these approaches allow the rule of law to be examined not only as a formal doctrine, but as a normative framework for evaluating digitally mediated governance.

In Dicey's conception, the rule of law rests on the supremacy of law over arbitrary power, equality before the law, and the protection of rights through ordinary courts (Dicey, 1945; Zabdyr-Jamróz, 2013). Although this account is frequently criticised for its formalism, it remains highly relevant in the digital environment. The expansion of automated and data-driven decision-making raises a question that is fundamentally Diceyan in character: who actually exercises power when decisions are produced or shaped by opaque technical systems, and under what legal conditions can that power be reviewed? In this sense, Dicey's theory remains useful because it identifies the first threshold of a digital rule of law: the exercise of power must remain legally attributable, reviewable, and limited.

Fuller approached the rule of law differently, not as mere formal legality but as the 'internal morality of law'. His eight principles – such as clarity, consistency, pub-

licity, and congruence between declared rules and official action – are especially relevant where governance is mediated by algorithmic systems (Fuller, 1978; Tokarczyk, 1978). From the perspective of this article, Fuller is important because digital systems often fail precisely where legality should be strongest: they may be difficult to understand, unstable, resistant to explanation, and inaccessible to those affected by them. Fuller therefore helps to show that the crisis triggered by algorithmic governance is not only about technological opacity; it is about whether decision-making arrangements still satisfy the minimum procedural conditions of legality.

Rawls adds a third dimension by linking the rule of law to procedural justice and the fair organisation of social institutions. In *A theory of justice* (1971), the rule of law appears as one of the conditions of a well-ordered society, that is, a society in which public power is exercised through publicly knowable and justifiable rules. In the digital context, this perspective becomes especially important when decisions are based on profiling, classification, or automated assessment. The Rawlsian question is no longer only whether a rule exists, but whether the institutional environment in which it operates preserves equal status, fair treatment, and meaningful access to rights. Rawls is therefore needed in an article on the digital rule of law because he makes visible the distributive and civic consequences of digital governance, especially where individuals are transformed into data profiles subject to differentiated treatment.

Despite the differences between these authors, their theories converge on one crucial point: power is legitimate only when it is exercised through norms and procedures that are not arbitrary, inaccessible, or unjustifiable. This convergence is especially important in the digital era, where the exercise of public and quasi-public power is increasingly distributed across hybrid constellations of state institutions, private platforms, automated systems, and contractual infrastructures. As De Gregorio (2021) argues in the context of digital constitutionalism, the digital space should no longer be seen merely as a neutral environment of communication, but as a domain in which new forms of power directly affect democracy and fundamental rights. A similar argument is developed by Celeste (2019, 2022), who treats digital constitutionalism as a framework for extending constitutional values to the digital ecosystem and for addressing the growing normative role of private online platforms.

This observation supports the central claim of the present article: the rule of law must now be reformulated in a way that addresses not only public authority in the classical sense, but also algorithmic and infrastructural forms of governance. This issue becomes even clearer when placed alongside theories of digital democracy. The literature usually distinguishes three models: representative, participatory, and deliberative. These are not mutually exclusive; rather, they illuminate different dimensions of democratic legitimacy under digital conditions.

The representative model is based on indirect political participation through elections and institutions of representation. In digital conditions, it includes tools for communication with representatives, access to parliamentary information, and

in some cases e-voting procedures. Yet digitalisation has not resolved the structural weaknesses of representative democracy. On the contrary, it often intensifies the tension between citizens' expectations of immediacy, responsiveness, and personalisation, and the slower, formalised logic of constitutional institutions.

The participatory model places emphasis on direct citizen involvement in decision-making; digital technologies may strengthen this model through online consultations, participatory budgeting, and legislative crowdsourcing. As Obrebska (2016) has shown, such instruments can deepen the local embeddedness of institutions, provided that they are designed in an inclusive and transparent manner. At the same time, digital participation should not be romanticised: participation mediated by technology may remain selective, unequal, or merely symbolic if it is not accompanied by safeguards against exclusion and asymmetries of influence.

The deliberative model is particularly important for the purposes of this article, because it makes it possible to evaluate not only whether citizens participate, but also under what communicative conditions democratic legitimacy is produced. Here the Habermasian perspective is indispensable. Habermas' concept of the public sphere does not merely describe a space of discussion; it provides a normative model in which legitimacy depends on the circulation of reasons under conditions of openness, reciprocity, and discursive equality. This is precisely why the Habermasian framework remains useful in the digital context. The key problem is not simply that public debate has moved online, but that digital platforms now structure the visibility, hierarchy, and circulation of arguments. In other words, they do not merely mediate communication: they actively organise the conditions of public reason.

From this angle, the central tension of digital democracy becomes clearer. Deliberation in digital environments is increasingly shaped by ranking systems, moderation mechanisms, recommender architectures, and business models oriented towards engagement rather than rational and critical debate. As a result, what appears to be a neutral technological infrastructure may in fact reshape the communicative preconditions of democracy itself. The Habermasian perspective is therefore important not as an abstract philosophical reference, but as a normative test: it allows one to ask whether digitally mediated communication still satisfies the requirements of inclusiveness, equality of voice, accessibility of information, and reason-giving. In this respect, the prerequisites for deliberative democracy in the digital sphere include first, limits on algorithmic dominance and second, conditions that protect the communicative autonomy of citizens (Łapaj, 2016). Conversely, their absence may deepen emotional polarisation and weaken the rational quality of democratic discourse (Fuchs, 2025).

At this point, the relevance of Suzor (2011) also becomes apparent. His analysis of rule enforcement in online communities shows that digital environments are governed not only by public law, but also by privately created and enforced normative orders. This is important for the present argument because it demonstrates that the

digital public sphere is shaped by hybrid regimes of governance in which contractual rules, platform sanctions, and technical architectures may perform functions analogous to legal regulation, while remaining outside the classical guarantees associated with the rule of law. This further reinforces the need to conceptualise the digital rule of law as a response to dispersed and partly privatised forms of power.

Seen in this way, the three models of digital democracy are not merely descriptive categories. They identify three different dimensions of legitimacy that become unstable under digital conditions: accountability in the representative model, inclusion in the participatory model, and the quality of public reason in the deliberative model. Read together with Dicey, Fuller, and Rawls, they provide the conceptual foundation for the argument developed in the following sections of this article. The next part therefore moves from the level of theory to the transformation of institutions themselves, examining how digitisation reshapes public administration, citizen–state relations, and the conditions under which democratic legality can still be maintained.

2. The digitisation of societies and the transformation of public institutions in the context of digital democracy

Digitisation is no longer merely a technological phenomenon; it is transforming the institutional and social conditions under which public power is exercised. Contemporary information societies increasingly operate through hybrid models of communication, administration, and governance, in which digital technology functions not only as a tool but also as a framework that structures relations between individuals, public institutions, and the state (Gajowniczek, 2015). For this reason, the digitisation of public institutions should be analysed not only in terms of efficiency or innovation, but also as a process that redefines the normative foundations of democratic governance.

This transformation is visible in the digitisation of public services, the expansion of e-administration, the development of e-government systems, and the emergence of new channels of interaction between citizens and institutions, such as e-consultations and digital reporting platforms. From an institutional perspective, the broader ambition of these processes has often been framed as the construction of a 'smart' state: adaptable, data-driven, and more responsive to citizens' needs (Oleński, 2018). Yet the significance of this development lies not only in modernising administration, but in altering the very form through which the citizen encounters public authority.

Indeed, the digital transformation of public institutions involves a shift from a classical bureaucratic logic to the logic of digital services (Adamczewski et al., 2017). State institutions increasingly function through interoperable systems, automated procedures, and data-based coordination. This means that the role of administration is no longer limited to carrying out individual acts in a conventional procedural

framework; it also consists in sorting, classifying, and processing citizens through digital infrastructures. In such a setting, the relationship between the citizen and the state is gradually transformed: the individual no longer confronts only an office or an official, but also interfaces, databases, and systems of automated assessment.

This shift is legally and normatively significant. In the classical administrative model, the citizen's position was shaped primarily through a formal decision attributable to a public authority and at least in principle accompanied by justification and review. In a digital environment, however, the decisive moment may occur earlier, at the level of data processing, automated pre-selection, or system-generated categorisation. As a result, the citizen may be governed not only through legal acts, but also through technical procedures that influence access to services, shape administrative priorities, and structure the practical possibility of exercising rights. From the perspective of the rule of law, this means that the focus can no longer rest exclusively on the final decision; attention must also be directed to the digital architecture through which the decision is prepared and operationalised. As digital platforms – from e-government portals to online banking – progressively replace in-person services, individuals who refrain from participating in digital environments may face increasing marginalisation. This development also prompts a further question: whether human rights law safeguards an individual's freedom to maintain an analogue way of life, and to what extent such a choice remains feasible in contemporary society (Kużelewska et al., 2025, p. 58).

At the same time, digitisation is not neutral in its social effects. As Kilias (2017) observes, the apparent transparency and rationality of technological systems may conceal a deepening of inequalities and the consolidation of asymmetrical access to power. If digital transformation is not accompanied by an adequate democratisation of procedural mechanisms, it may lead not to a more transparent state, but to the technocratisation of governance. In such a model, efficiency is privileged over explanation, and automation over accountability.

This danger is especially visible in the case of Central and Eastern European countries, including Poland, where the digitisation of public administration has often been fragmented, strongly technology-oriented, and insufficiently grounded in participatory values. In these conditions, digitisation may produce what can be called e-bureaucracy: not the substantive transformation of administration, but the digital reproduction of existing hierarchies and rigidities. The result is a paradox in which institutions become more technologically advanced without necessarily becoming more transparent, accessible, or responsive.

Digitisation also transforms social expectations towards the state. Citizens increasingly perceive institutions as permanent service providers and expect immediacy, personalisation, and intuitive access. This marks a broader change in the experience of public authority: the state is no longer judged solely by legality in the formal sense, but also by usability, speed, and informational clarity. Yet this shift also

creates tension. A faster and more personalised administration is not necessarily a more lawful one. The challenge is therefore not simply to digitalise institutions, but to ensure that the service-oriented logic of digitisation remains compatible with the legal guarantees traditionally associated with public administration.

Estonia is frequently invoked as an example of successful digital transformation. Its significance lies both in its implementation of advanced e-government solutions and in the broader combination of technology, institutional trust, and legal stability (Szwed, 2018). The Estonian example suggests that the effectiveness of digitisation depends not merely on technical capacity, but on the existence of a stable normative environment in which citizens trust institutions and institutions remain accountable in their use of digital tools. This is important for the argument here, because it shows that digital transformation strengthens democracy only when it is embedded in a broader framework of legality and public trust.

Concurrently, digitisation has enabled new forms of civic engagement, including electronic voting systems, consultation platforms, and online tools of direct participation. These instruments may broaden participation and facilitate access to public processes, but they also require digital competence, institutional credibility, and robust safeguards for data security (Gajowniczek, 2015). Their democratic value therefore depends less on their technical availability than on the extent to which they generate meaningful inclusion rather than merely symbolic participation.

It is also necessary to situate these developments within the framework of European Union law. Digital states do not operate in a normative vacuum but under legal conditions increasingly shaped by instruments such as the DSA, the AI Act, and the GDPR. These regulations introduce standards of transparency, proportionality, data protection, and accountability that are directly relevant to the digital exercise of public power. At the same time, as Fischman-Afori (2022) suggests, the effectiveness of these legal frameworks depends on institutional readiness to implement mechanisms for control, oversight, and audit. Regulation alone is therefore insufficient unless public institutions are capable of translating formal obligations into actual procedural guarantees.

For this reason, the digitisation of societies and public institutions should be understood as an axiological and systemic transformation rather than merely an infrastructural one. The central issue is no longer whether public institutions should be digitised, but under what conditions digitisation can reinforce rather than weaken democratic legitimacy. The key problem is whether technology remains a tool supporting legality, participation, and accountability, or whether it gradually becomes a medium through which public power escapes classical forms of control. This question provides the bridge to the following parts of this article, which examine both the democratic opportunities created by digital technologies and the risks they pose to the rule of law.

3. Digital technologies as an opportunity for democracy and the rule of law

The digital transformation of contemporary societies poses serious challenges to democratic institutions, but it also creates opportunities to strengthen transparency, accountability, and inclusion. These opportunities should not be understood in purely technological terms. Digital tools do not enhance democracy automatically; they can do so only when they are embedded in legal and institutional frameworks that preserve procedural fairness, public oversight, and effective access to rights. From this perspective, three areas are of particular importance: e-democracy, open data combined with the automation of procedures, and blockchain-based infrastructures.

E-democracy encompasses a broad spectrum of digitally mediated forms of civic participation, ranging from online voting and public consultations to instruments supporting deliberative democracy. Its democratic potential lies in lowering barriers to participation and widening access to legislative and administrative processes. In Poland, however, development in this area remains gradual and continues to depend heavily on questions of security and public trust. Research indicates that although the idea of electronic voting enjoys considerable social acceptance, its legitimacy depends on robust guarantees of transparency, auditability, and procedural reliability (Lubik-Reczek et al., 2020). This is crucial from the perspective of the rule of law: broadening participation is normatively valuable only if the procedures through which participation is organised remain verifiable and contestable.

A similar logic applies to public consultations conducted electronically. Digital consultation systems may increase transparency and widen participation in the legislative process, but their democratic value depends on their institutional design. If they are properly moderated and linked to actual decision-making processes, they may function as meaningful tools of co-decision rather than instruments of a symbolic consultation (Harasimiuk & Braun, 2021). At the same time, as Brusseau (2021) argues, the growing role of automated systems in participatory environments requires renewed ethical reflection, especially in relation to data protection, inclusion, and the risk of unequal influence. The problem is therefore not the mere existence of digital participation tools but whether they create real conditions for democratic agency.

The second area concerns open data and the automation of procedures. In democratic systems, transparency and administrative effectiveness increasingly depend on the availability of public information and on the capacity of institutions to process data in a timely and coherent way. Open data may strengthen public oversight, facilitate the monitoring of institutions by civil society and the media, and reduce opportunities for abuse (Matheus et al., 2021). In Poland, however, the development of open data infrastructures still faces important limitations, especially in terms of interoperability and standardisation (Dudarski, 2024). This means that the democratic

potential of transparency is often constrained not by a lack of formal commitments but by institutional fragmentation.

At the same time, the automation of administrative procedures, including the use of artificial intelligence in public administration, may improve accessibility to services and reduce the duration of proceedings, provided that mechanisms for explanation, review, and appeal are preserved. If such guarantees are absent, automation may come into conflict with the principles of legality and the right of defence. This issue is particularly visible in the field of public finance control, where digital technologies and AI-based tools may strengthen the capacity of the state to detect irregularities and improve oversight of public expenditure (Skuza & Lizak, 2023). The significance of such solutions lies not only in their technical efficiency, but also in the possibility of increasing institutional accountability. Yet this promise remains conditional: automation strengthens the rule of law only when the systems used by public institutions remain transparent enough to be scrutinised and procedurally structured enough to be challenged.

The third area is blockchain technology, which is frequently presented as a tool capable of enhancing transparency, consistency, and accountability. In the public sphere, its potential applications include electronic voting, administrative records, and the management of public registers (Szostek et al., 2025). From a legal and institutional perspective, the attraction of blockchain lies in its capacity to reduce information asymmetries and make certain forms of record-keeping more resistant to manipulation (Chmielarz, 2025). For this reason, it is sometimes described as an instrument that could strengthen public trust, especially in areas such as public finance, registries, or transactional integrity.

At the same time, blockchain should not be treated as a self-sufficient source of legitimacy. As De Filippi and Wright (2020) note, blockchain-based systems may operate as a form of *lex cryptographia*, that is, a normative order embedded in code and enforced through protocol. While such an architecture can increase certainty and automatise compliance, it also raises difficult questions about flexibility, contestability, and the legitimacy of norms that are embedded in technical design rather than generated through democratically accountable procedures. In the context of this article, the importance of blockchain therefore lies not in its technological novelty as such, but in the fact that it makes the broader problem of the digital rule of law particularly visible: the growing transfer of norm-setting and norm-enforcement functions from legal institutions to technical infrastructures.

For this reason, the democratic opportunities created by digital technologies should be used with caution. E-democracy, open data, procedural automation, and blockchain-based systems may all contribute to stronger democratic governance, but only if they remain subordinated to the requirements of legality, accountability, transparency, and effective review. Otherwise, the same technologies that promise

inclusion and control may instead produce new forms of opacity, dependency, and exclusion.

4. Digital democracy and the rule of law: Threats and challenges

The ongoing digitisation of social life and the growing use of computing technologies by public institutions raise fundamental questions about the future of the rule of law, transparency, and the accountability of public authorities. From the perspective of this article, four interrelated threats are of particular importance: algorithmic discrimination, disinformation and manipulation, mass surveillance, and the crisis in decision-making accountability. These phenomena should not be treated as isolated technological failures; rather, they reveal structural tensions between the logic of digital systems and the legal principles on which democratic governance is based.

The first threat is algorithmic discrimination. Contemporary decision-making systems increasingly rely on machine-learning models trained on historical data and statistical predictions. Although they are often introduced in the name of efficiency, these systems may reproduce and intensify existing social biases, especially in areas such as recruitment, profiling, selection, and the allocation of benefits (Mazur, 2021). It has been widely observed that artificial intelligence systems tend to replicate the patterns embedded in the data on which they are trained, including discriminatory assumptions and historically unequal treatment (Barocas & Selbst, 2016; Eubanks, 2018). The problem therefore extends beyond technical error: it concerns the compatibility of automated decision-making with equality before the law. Where the logic of prediction replaces individualised legal assessment, traditional guarantees of the rule of law – such as the right to know the reasons for a decision and the effective possibility of appeal – become more difficult to realise. From this perspective, the opacity of predictive systems is not merely a technical inconvenience; it is a direct challenge to legality and procedural justice. For this reason, it is necessary to develop legal mechanisms that ensure transparency, auditability, and the possibility of contesting decisions produced or shaped by automated systems (Citron & Pasquale, 2014). The spread of AI-based systems also requires a reconsideration of both administrative and criminal liability, including the responsibility of those who design, deploy, and use such systems in public contexts (Skowrońska, 2024).

The second threat concerns disinformation and manipulation in the digital public sphere. Digital democracy undoubtedly expands the capacity for communication, but it also creates favourable conditions for the rapid dissemination of false or misleading content. Disinformation and deepfakes weaken trust in institutions, disrupt public deliberation, and may distort electoral processes (Gruszko, 2021). At the same time, the recommendation logics used by social media platforms tend to privilege content that is emotionally engaging, polarising, or sensational, thereby contributing

to social fragmentation. The role of platforms in the amplification of falsehoods, polarisation, and the erosion of rational discourse has been extensively discussed in the literature (Tucker et al., 2018; Zuboff, 2019). From the perspective of the rule of law, the central issue is whether citizens retain reliable access to information of sufficient quality to make informed political choices. When visibility is organised according to the logics of data extraction and selective amplification, the public sphere ceases to function as a neutral environment of communication and instead becomes a space of asymmetrical influence. In this sense, the digital public sphere, while formally open, increasingly operates according to a regime of selective visibility that constrains rational discourse and weakens the epistemic foundations of democracy (Płonowska-Ziarek, 2021).

The third threat is mass surveillance and the broader asymmetry of informational power. Digital technologies have enabled an unprecedented degree of monitoring in both the public and private spheres. Mass data collection, behaviour tracking, predictive analytics in administration, and surveillance-oriented technologies in law enforcement and justice all weaken the constitutional guarantees of privacy and informational self-determination (Skowrońska, 2024). These developments correspond to what has been described as a 'black-box society', in which the individual becomes increasingly transparent to institutions while remaining unable to understand the systems through which s/he is observed, classified, or evaluated (Gruszko, 2021). A related problem is that citizens often lose meaningful control over how their data is processed and for what purposes it is used, despite the existence of formal guarantees under the GDPR. From a human rights perspective, this means a deterioration not only of privacy, but also of freedom of communication and anonymity in the public space. Technologies such as facial recognition, geolocation, and behaviour analysis create imbalances of knowledge and power that may bypass ordinary mechanisms of democratic oversight (Green & Viljoen, 2020). Moreover, digitalisation may generate a more subtle form of coercion: the practical impossibility of opting out of digital infrastructures in areas essential to everyday life. As has been argued in the context of financial markets, the right to remain outside digital systems may become increasingly fictional when access to basic services depends on technological participation (Nieborak, 2025). This insight is relevant beyond the financial sector because it highlights how digital dependence may transform formal freedom into a constrained and unequal choice.

The fourth threat is the crisis in decision-making accountability. One of the core principles of the rule of law is that public decisions must be attributable to identifiable authorities and open to review. Yet when decision-making is mediated by opaque algorithmic systems, responsibility becomes diffuse and difficult to reconstruct. Citizens may find it impossible to challenge decisions whose source, logic, or chain of responsibility cannot be clearly identified (Gruszko, 2021). The absence of comprehensible justification for AI-assisted decisions represents not only a technological

difficulty but also a constitutional problem, because it weakens judicial scrutiny and undermines the principle of effective legal protection (Kroll et al., 2017). As a consequence, the classical model of administrative and political accountability is increasingly destabilised. The automation of public power creates situations in which the actual decision-maker becomes institutionally invisible, thereby complicating both legal and ethical responsibility (Płońska-Ziarek, 2021). What is at stake here is not only who makes the decision, but whether the citizen can still confront public authority in a legally meaningful way.

Taken together, these four threats show that the digital transformation of democratic institutions requires more than technical adaptation. Algorithmic inequality, disinformation, ubiquitous surveillance, and the opacity of automated decision-making all reveal the need to reinterpret the core principles of the rule of law under digital conditions. They are not external side effects of technological progress but structural challenges to the political and legal order. For this reason, the central question is no longer whether digital technologies should be used in democratic governance, but under what normative conditions their use remains compatible with legality, transparency, accountability, and fundamental rights. This conclusion provides the basis for the next part of the article, which turns from diagnosis to normative proposals and examines how the concept of a digital rule of law might be operationalised.

5. Digital democracy and the rule of law: Normative proposals and recommendations

The rapid development of digital technologies and the growing influence of platforms on public communication have led to the emergence of the concept of digital constitutionalism, understood as an attempt to extend constitutional principles to the digital environment. At its core lies the assumption that the values traditionally associated with the rule of law – legality, transparency, accountability, and the protection of individual rights – must also structure digital architectures and platform-based governance (Granat, 2022). In this sense, digital constitutionalism is not limited to protecting users against private abuse; it also serves as a broader framework for legitimising digital decision-making processes, including content moderation, algorithmic selection, and the infrastructural conditions under which political communication becomes visible, amplified, or marginalised (Piotrowski, 2023). Challenges such as behaviour prediction, voter profiling, and algorithmic moderation therefore require more than isolated sectoral interventions: they call for a systematic rethinking of the relationship between law, public power, and technical infrastructures.

From this perspective, a digital rule of law should be understood as a normative programme aimed at ensuring that digital governance remains compatible with constitutional standards. This requires not only the adaptation of existing legal institu-

tions, but also the development of procedures capable of addressing forms of power that are exercised through code, data processing, and platform design. In practical terms, this means that the constitutionalisation of the digital sphere must reach beyond declarations of principle and take institutional form.

A central element of this process is the regulation of artificial intelligence. The AI Act has been adopted as Regulation (EU) 2024/1689, establishing a risk-based framework for AI systems within the European Union. Its significance lies in the fact that it seeks to intervene before rights violations occur, which distinguishes it from more traditional *ex post* mechanisms of constitutional protection (Harasimiuk & Braun, 2021). The Regulation prohibits certain AI practices regarded as incompatible with Union values and fundamental rights (Art. 5 AI Act), classifies certain systems as high-risk (Art. 6 and Annex III AI Act), and imposes obligations concerning risk management, data governance, transparency, human oversight, and technical robustness (Arts. 9–10, 13–15 AI Act). In this respect, the Act reflects an important shift: it recognises that legality in the digital sphere cannot depend solely on the review of outcomes after the fact, but must also shape the design and deployment of systems in advance.

This regulatory framework should be read together with the broader ethical and legal debate on AI. Ethical guidelines, such as those prepared by the European Commission's High-Level Expert Group on AI, emphasise transparency, accountability, non-discrimination, and human oversight (Floridi et al., 2018). Yet a persistent problem is the gap between these normative principles and the operational logic of many commercial and institutional systems, especially where black-box algorithms remain difficult to scrutinise and practically inaccessible to public control. For this reason, the regulation of AI cannot be confined to technical compliance alone; it must also include procedural guarantees that protect the individual against opaque and unchallengeable decisions. Where automated systems affect someone's legal status, access to services, or participation in public life, the minimum requirements of the digital rule of law should include the right to meaningful information, the possibility of human review, and access to effective remedies.

A similar logic applies to the Digital Services Act, which is central to the regulation of platforms' power and of digital public discourse. It introduces procedural safeguards that are particularly important from the perspective of democratic legitimacy and the rule of law. These include the obligation to provide statements of reasons for certain moderation decisions (Art. 17 DSA), access to internal complaint-handling systems (Art. 20 DSA), and specific obligations concerning recommender systems and the mitigation of systemic risks in very large online platforms (Arts. 27, 34–35 DSA). These provisions are significant because they move regulation beyond the abstract protection of users and towards procedural control over the infrastructures that shape digital visibility and political communication. Nevertheless, even these measures do not fully resolve the deeper structural tension between legal

rationality and algorithmic governance. They improve oversight but do not eliminate the asymmetry between those who design and operate digital systems and those who are subject to them.

For this reason, a digital rule of law must be operationalised through a set of concrete institutional requirements. At a minimum, this should include a clear legal basis for the use of algorithmic systems by public authorities; mandatory *ex ante* assessments of their impact on fundamental rights; the documentation and auditability of the data, models, and decision-making logic used; meaningful human oversight over automated outcomes; and accessible procedures through which individuals can obtain reasons, challenge decisions, and seek review by an independent body. In addition, public authorities should maintain transparency registers for high-risk algorithmic systems used in administration. Without such safeguards, digital regulation risks remaining declaratory rather than transformative.

The final pillar of this normative architecture concerns the expansion of citizen participation in lawmaking through digital tools. Many states have introduced e-consultation platforms, online participatory budgets, and electronic participation mechanisms. Yet, as noted in the literature, these forms of participation are often merely advisory and do not substantially influence final decisions (Obrebska, 2016). If digital participation is to contribute to democratic legitimacy, it must go beyond symbolic consultation and become connected to actual institutional effects. This is why the idea of collaborative lawmaking is particularly relevant: it refers to procedures in which citizens are not only invited to comment on ready-made drafts, but are involved earlier in the consultation on and formulation of legislative proposals. Examples from Barcelona, Iceland, and Finland show that such models are institutionally possible and can serve as points of reference for broader European implementation (Hoven et al., 2024). Their success, however, depends less on digital accessibility alone than on whether they are genuinely inclusive, socially representative, and capable of influencing legal outcomes (Fuchs, 2025).

In this context, digital participation should itself be subject to rule-of-law criteria. Participation procedures must be transparent, intelligible, and resistant to manipulation, and citizens should know how their input is processed, whether it has influenced the final outcome, and according to which criteria contributions have been selected, prioritised, or rejected. Otherwise, participation risks becoming an instrument that merely appears to be democratic rather than being truly legitimate.

The advancement of digitalisation therefore requires a deeper normative reflection on the role of technology within democratic states. The three directions discussed in this section – digital constitutionalism, the legal and ethical regulation of AI, and the strengthening of collaborative digital participation – should be treated as complementary elements of a broader project of constitutionalising the digital sphere. Only under these conditions can technology serve as an instrument of democracy rather than a substitute for it. In this sense, a digital rule of law should be understood not as

a metaphor but as a concrete institutional model whose minimum content includes legality, transparency, auditability, human oversight, and effective remedies in all areas where digital systems shape rights, obligations, and public discourse.

Conclusions

Digital democracy is not merely a technological extension of existing institutions. It transforms the conditions under which public power is exercised, public discourse is structured, and citizens participate in democratic life. The analysis conducted in this article confirms that the classical model of the rule of law, developed under the conditions of analogue democracy, is insufficient in the face of platforms' power, algorithmic opacity, and automated decision-making. Therefore the concept of a digital rule of law should be treated as a necessary normative response rather than as a descriptive metaphor.

This article has shown that digital technologies may strengthen transparency, participation, and administrative effectiveness, but only under clearly defined legal and institutional conditions. In the absence of such conditions, digitalisation is more likely to deepen existing asymmetries than to democratise governance. Algorithmic discrimination, disinformation, mass surveillance, and the diffusion of responsibility in automated systems are not peripheral risks; they are structural challenges to legality, accountability, and the effective protection of fundamental rights.

The key conclusion is that a digital rule of law must be operationalised through concrete safeguards. Its minimum institutional content should include a clear legal basis for the use of algorithmic systems by public authorities; transparency concerning such systems' existence, purpose, and effects; the auditability of high-risk systems; meaningful human oversight; the right to obtain reasons for decisions affecting individuals; and access to effective review by an independent body. In particular, the auditability of public algorithms should be treated as a *sine qua non* condition of a digital rule of law.

This article also demonstrates that existing EU instruments, including the DSA, the GDPR, and the AI Act, constitute important elements of an emerging legal framework for digital governance. However, their effectiveness depends not only on their formal adoption, but on an institutional capacity to enforce them and on the availability of real procedural guarantees for citizens. Regulation alone is not sufficient if digital systems remain practically opaque and insulated from review.

A further conclusion concerns democratic participation. Digital tools can support inclusion and improve access to lawmaking processes only if participation is transparent, procedurally meaningful, and linked to actual influence over public decisions. Otherwise, digital participation risks becoming merely symbolic and may serve to legitimise decisions already shaped elsewhere.

Ultimately, the decisive question is not whether democracy will continue to digitalise, but whether digitalisation will remain subject to the normative discipline of the rule of law. If technological infrastructures are left opaque, unreviewable, and weakly accountable, democracy in the algorithmic age may drift towards technocratic governance without effective civic control. If, however, digital systems are embedded in a framework of legality, transparency, accountability, and participation, they may strengthen rather than weaken the democratic order. The future of democracy therefore depends on whether a digital rule of law can be developed, not only as a concept but also as an enforceable institutional practice.

REFERENCES

Adamczewski, P., Matusiak, J., Mielczarek, J., Nowak, P. A., Przywojska, J., & Szydłowski, C. (2017). *Innowacje 2017. Rozwój społeczeństwa informacyjnego w Polsce*. Urząd Marszałkowski Województwa Łódzkiego. http://hdl.handle.net/11089/23865

Barocas, S., Selbst, A.D. (2016). *Big data's disparate impact*. Calif. L. Rev., 104, 671–732

Brusseau, J. (2021). AI, democracy, and the ethics of online voting. *AI and Ethics*, *2*, 441–447. https://doi.org/10.1007/s43681–021–00090-z

Caruso, C. (2025). Towards the institutions of freedom: The European public discourse in the digital era. *German Law Journal*, *26, 114–137*. https://doi.org/10.1017/glj.2024.68

Celeste, E. (2019). Digital constitutionalism: A new systematic theorisation. *International Review of Law, Computers & Technology*, *33*(1), 76–99. https://doi.org/10.1080/13600869.2019.1562604

Celeste, E. (2022). *Digital constitutionalism: The role of internet bills of rights*. Routledge. https://doi.org/10.4324/9781003256908

Chmielarz, P. (2025). Blockchain jako narzędzie transparentności wydatków jednostki samorządu terytorialnego – weryfikacja transakcji w czasie rzeczywistym. *Rocznik Administracji Publicznej*, *11*(2), 417–442. https://doi.org/10.4467/24497800RAP.25.043.22558

Citron, D. K., & Pasquale, F. (2014). *The scored society: Due process for automated predictions*. Wash. L. Rev., 89, 1

De Filippi, P., & Wright, A. (2020). Decentralized blockchain technology and the rise of lex cryptographia. *SSRN Electronic Journal*. http://dx.doi.org/10.2139/ssrn.2580664

De Gregorio, G. (2021). *Constitutional law in the information society: Protecting fundamental rights and democracy in the age of artificial intelligence* [Doctoral dissertation, University of Milano-Bicocca]. https://boa.unimib.it/handle/10281/305226

Dicey, A. V. (1945). *An introduction to the study of the law of the constitution*. Macmillan.

Dudarski, Ł. (2024). Cyfryzacja administracji publicznej w Polsce: wyzwania i perspektywy. *Zeszyty Naukowe Collegium Witelona*, *4*(53), 57–70. https://doi.org/10.5604/01.3001.0055.2334

Eubanks, V. (2018). *Automating inequality: How high-tech tools profile, police, and punish the poor.* Macmillan+ ORM.

Fischman-Afori, O. (2022). Global digital governance through the back door of corporate regulation. *Fordham Intellectual Property, Media & Entertainment Law Journal*, *33*(3), 1–44. https://dx.doi.org/10.2139/ssrn.4215774

Floridi, L., Cowls, J., Beltrametti, M., Chatila, R., Chazerand, P. Dignum, V., Luetge, C., Madelin, R., Pagallo, U., Rossi, F., Schafer, B., Valcke, P. & Vayena, F. (2018). AI4People – An ethical framework for a good AI society: Opportunities, risk, principles, and recommendations. *Minds and Machines*, *28*, 689–707. https://doi.org/10.1007/s11023–018–9482–5

Fuchs, C. (2025). What is and how do we achieve a resilient digital democracy? *Open Research Europe*, *5*, 387. https://doi.org/10.12688/openreseurope.21988.1

Fuller, L. L. (1978). *Moralność prawa*. Państwowy Instytut Wydawniczy.

Gajowniczek, T. (2015). Elektroniczna demokracja – istota pojęcia i problemy definicyjne. In W. Tomaszewski, D. M. Mościcka, & A. Jurkun (Eds.), *Demokracja a wybory. Współczesne dylematy i wyzwania* (pp. 11–30). Instytut Nauk Politycznych UWM.

Granat, M. (2022). Pytania o przyszłość konstytucjonalizmu. Siła i słabość komparatystyki prawniczej. *Przegląd Konstytucyjny*, *2*, 33–46. https://doi.org/10.4467/25442031PKO.22.020.16385

Green, Ben & Viljoen, Salomé. (2020). *Algorithmic realism: expanding the boundaries of algorithmic thought*. In Proceedings of the 2020 Conference on Fairness, Accountability, and Transparency (FAT* '20). Association for Computing Machinery, New York, NY, USA, 19–31. https://doi.org/10.1145/3351095.3372840

Gruszko, K. (2021). *Prawo do informacji w społeczeństwie czarnej skrzynki*. Zatruta Studnia? Media w Czasach Pandemii COVID-19. https://www.academia.edu/45131798/Gruszko_Prawo_do_informacji_w_spo%C5%82ecze%C5%84stwie_czarnej_skrzynki

Harasimiuk, D. E., & Braun, T. (2021). Nowa złożoność. Dialog demokratyczny w warunkach transformacji cyfrowej. *Przegląd Konstytucyjny*, *4*, 60–92.

Hoven, J., Stauch, M., Musiani, F., Domingo-Ferrer, J., Ruggieri, S., Pratesi, F., Trasarti, R., & Comandé, G. (2024). *Democracy in the digital age*. https://shs.hal.science/halshs-04844505v1

Kilias, J. (2017). Wprowadzając ponownie państwo: od socjologii historycznej do państwocentrycznej. In J. Raciborski (Ed.), *Państwo w praktyce: style działania* (pp. 65–84). Nomos.

Kroll, J. A., Huey, J., Barocas, S., Felten, E. W., Reidenberg, J. R., Robinson, D. G., & Yu, H. (2017). Accountable algorithms. *University of Pennsylvania Law Review*, 165(3), 633–705.

Kużelewska, E., Malinowski, D., & Tomaszuk, M. (2025). Human rights and digital choice: Rethinking the right (not) to use the internet. *Białostockie Studia Prawnicze*, *30*(4), 57–71. https://doi.org/10.15290/bsp.2025.30.04.04

Łapaj, J. (2016). Demokracja deliberatywna – zalety i zastrzeżenia wobec modelu w kontekście rozważań. In A. Turoń-Kowalska (Ed.), *Demokracja deliberatywna: utopia czy ratunek dla demokratycznych wartości?. Remar, 137–154.*

Lubik-Reczek, N., Kapsa, I., & Musiał-Karg, M. (2020). *Elektroniczna partycypacja obywatelska w Polsce. Deklaracje i opinie Polaków na temat e-administracji i e-głosowania*. UAM-WNPiD.

Matheus, R., Janssen, M., & Janowski, T. (2021). Design principles for creating digital transparency in government. *Government Information Quarterly*, *38*(1). https://doi.org/10.1016/j.giq.2020.101550

Mazur, J. (2021). *Algorytm jako informacja publiczna w prawie europejskim*. Wydawnictwa Uniwersytetu Warszawskiego.

Nieborak, T. (2025). Digital coercion? The financial market and the right to digital opt-out between fiction and reality. *Białostockie Studia Prawnicze*, *30*(4), 119–136. https://doi.org/10.15290/bsp.2025.30.04.08

Obrebska, M. (2016). Wprowadzenie i rozwój budżetu partycypacyjnego w angielskim samorządzie lokalnym. In A. Turoń-Kowalska (Ed.), *Demokracja deliberatywna: utopia czy ratunek dla demokratycznych wartości?*. Remar, 137–154.

Oleński, J. (2018). Strategie rozwoju e-państwa w perspektywie 2030 roku. *Roczniki Kolegium Analiz Ekonomicznych*, *48*, pp. 83–120.

Pane, S. (2025). The European 'post-digital' public sphere: Foundations of an emerging paradigm in the social sciences. *Methaodos: Revista de Ciencias Sociales*, *13*(1). https://doi.org/10.17502/mrcs.v13i1.866

Piotrowski, R. (2023). Konstytucjonalizm a tożsamość państwa demokratycznego. *Przegląd Konstytucyjny*, *3*, 7–23. https://doi.org/10.4467/25442031PKO.23.015.18562

Płonowska-Ziarek, E. (2021). Rządy ludzkie czy algorytmiczne? O automatyzacji władzy sądzenia. *teksty drugie*, (6), 237–252.

Rawls, J. (1971). *A theory of justice*. Harvard University Press. https://doi.org/10.2307/j.ctvjf9z6v

Schlag, G. (2023). European Union's regulating of social media: A discourse analysis of the DSA. *Politics and Governance*, *11*(3). https://doi.org/10.17645/pag.v11i3.6735

Skowrońska, J. (2024). *Prawnokarne aspekty technologii wykorzystującej sztuczną inteligencję ze szczególnym uwzględnieniem kwalifikacji prawnej, przypisaniem sprawstwa i odpowiedzialności twórcy* (rękopis). Uniwersytet Łódzki. Wydział Prawa i Administracji. https://www.bip.uni.lodz.pl/file-admin/user_upload/mgr_Julita_Skowro%C5%84ska_praca_doktorska.pdf

Skuza, S., & Lizak, R. (2023). Sztuczna inteligencja umożliwia kontrolę finansów publicznych – przegląd inicjatyw amerykańskiego rządu federalnego. *Białostockie Studia Prawnicze*, *28*(2,), 175–195. https://doi.org/10.15290/bsp.2023.28.02.11

Suzor, N. (2011). Order supported by law: The enforcement of rules in online communities. *Mercer Law Review*, *63*(1), 523–588.

Szostek, D., Malarewicz-Jakubów, A., & Castellani, M. (2025). Koncepcja i podstawy prawne dla nowego ujęcia rejestru – 'Rejestr 3.0'. *Białostockie Studia Prawnicze*, *30*(3), 181–195. https://doi.org/10.15290/bsp.2025.30.03.12

Szwed, K. (2018). Pozycja ustrojowa rządu Estonii oraz jego rola w tworzeniu nowoczesnego państwa. *Polityka i Społeczeństwo*, *2*(16), pp. 83–98. http://dx.doi.org/10.15584/polispol.2018.2.6

Tokarczyk, R. (1978). Koncepcja proceduralnego prawa natury Lon L. Fullera. *Annales Universitatis Mariae Curie-Skłodowska*, *25*(15), 225–244.

Tucker, J. A., Guess, A., Barbera, P., Vaccari, C., Siegel, A., Sanovich, S., & Nyhan, B. (2018). *Social media, political polarization, and political disinformation: A review of the scientific literature* (March 19, 2018). SSRN Electronic Journal.

Zabdyr-Jamróz, M. (2013). Zasada rządów prawa w koncepcji Alberta Venn Dicey'a. *Politeja. Pismo Wydziału Studiów Międzynarodowych i Politycznych UJ*, *23*, 311–343.

Zuboff, S. (2019). Surveillance Capitalism and the Challenge of Collective Action. *New Labor Forum*, 28(1), 10–29.