UNIVERSITY OF BIALYSTOK
FACULTY OF LAW

BIALYSTOK LEGAL STUDIES

BIAŁOSTOCKIE STUDIA PRAWNICZE

BIAŁYSTOK 2026 VOLUME 31 no. 1

BIALYSTOK LEGAL STUDIES
BIAŁOSTOCKIE STUDIA PRAWNICZE

VOLUME 31 no. 1

The original version of the journal is a print one.

ISSN 1689–7404
e-ISSN 2719–9452

Volume Theme Editors: David Ramiro Troitino & Viktoria Mazur, Tallinn Technology Uniwersity, Estonia

Language Editors: Claire Taylor-Jay

Statistical Editor: Ewa Glińska

Graphic and Typographic Development: Eliza Wasilewska, Jerzy Banasiuk

Cover Design: Bogusława Guenther

Publisher: Faculty of Law, University of Białystok; Temida 2

All volumes can be purchased from Wydawnictwo Temida 2. Address: ul. A. Mickiewicza 1, 15-213 Białystok, Poland. E-mail: temida2@uwb.edu.pl, Tel. +48 85 745 71 68

Contens

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.

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

sciendo

DOI: 10.15290/bsp.2026.31.01.02

Received: 24.08.2025
Accepted: 13.12.2025

Arianna Maceratini
University of Macerata, Italy
arianna.maceratini@unimc.it
ORCID ID: 0000–0001–7519–9016

The Digital Agora: Emerging Technologies, Freedom of Information and Democratic Space

Abstract: The digital revolution, fuelled by information technologies, has profoundly transformed the perception of reality and subjective interactions, with significant political, legal, social and economic implications. Current communication technologies hold a pervasive, often opaque, computational power that develops in virtual contexts in which the individual merges with the digital environment. In this scenario, the risk is that algorithmic solicitations, based on in-depth knowledge of individual habits, produce a form of hidden governance of choices, accentuating the information asymmetry between users and digital service providers. The contemporary world, defined by data correlations and algorithmic selections, thus takes on the characteristics of a 'black-box society', in which the distinction between the state and the market is blurred, new forms of surveillance emerge, and democratic principles and the rule of law are called into question. In the absence of defined spatial boundaries, regulatory divergences between the United States and Europe on the right to freedom of expression highlight the need to harmonize different legal and cultural visions. Therefore a global regulatory approach is proposed that can integrate human values into algorithms and promote digital education as a tool to increase civic awareness and collective responsibility in the information ecosystem.

Keywords: computational power, digital information, right of expression, democracy, rule of law

Introduction

The informational revolution, generated and fuelled by digital technologies, has profoundly transformed our perception of reality and the dynamics of human interactions, with wide-ranging political, legal, social and economic implications (Floridi, 2012). This evolution has given rise to an 'infosphere' populated by both natural and

artificial informational agents capable of autonomously collecting and processing data (Floridi, 2017). Within this infosphere, the virtualization of reality redefines value: access to digital information now complements, and often exceeds, the importance of owning material goods, revealing a shift toward the immateriality of what is exchanged (Amato Mangiameli & Campagnoli, 2020; Han, 2022; Rifkin, 2001). In this context, contemporary information and communication technologies exercise a subtle yet pervasive computational power (Durante, 2019), shaping a virtual dimension in which individuals become part of the environment itself, experiencing an 'onlife' continuity between the digital and the analogue worlds (Floridi, 2017, p. 53).

The construction of the individual as an informational system leads to a proxy culture driven by vicarious or indirect data that establishes correlations between information and predictions that are often *contra legem* and discriminatory (O'Neil, 2017, p. 28). This functions from the perspective of the personalization of performance, through which the individual is understood first and foremost as a consumer (Rifkin, 2001, p. 65), using recommendation systems driven by profit motives which may differ from the values developed by a genuinely democratic discourse (Habermas, 2023). So even if algorithms seem to operate for a neutral implementation of personal satisfaction, there is no objectivity in the filtering or in the personalization of information (Thurman et al., 2013); instead, they work with users in a 'co-productive manner' (Jasanoff, 2004) and, as they are made by humans, they could be fallible and spoiled by many prejudices. In addition, algorithms progressively narrow subjective action, reducing it to a sum of choices and preferences already expressed. The result is crystallized thought, a procedure that solves problems through codified steps, excluding spontaneity and the unexpected (Han, 2022, pp. 11, 53–54; Talia, 2018, p. 98), and highlighting several critical issues connected to the lack of transparency in the use of the criteria that define the output, which result in inadequate information being provided to the public (Amato Mangiameli, 2019; Palazzani, 2020; Zambonelli, 2020). In these circumstances, the risk is that suggestions become so performant as to establish a kind of hidden government of choice (Zambonelli, 2020, p. 66); in fact, although it is still the subject who decides on circumscribed aspects of the virtual experience, the outcome of the latter appears to be determined mainly by the algorithm. This amplifies, with unprecedented strength, the traditional nexus between knowledge, surveillance and power (Foucault, 1975), but from another perspective – that is, through a *smart* power that through algorithmic opacity makes the individual transparent, and that does not order but subtly induces the optimization of behaviour and the control of actions (Han, 2023, pp. 9–11), structuring a relevant information asymmetry between internet provider, digital platforms and the user of online services (Perri, 2020, pp. 17–18).

This essay examines some problematic nodes of the 'virtual agora' through the lens of algocracy, that is, the power of algorithms and the platforms that deploy them, focusing on their impact on freedom of information in the democratic space. From

a philosophical-legal perspective, it argues that only by intertwining normative and ethical-political dimensions can the complexity of digital transformations in public discourse be grasped: in this regard, rather than proposing a new theoretical model, the paper offers some critical reflections that invite a rethinking of traditional paradigms through algorithmic mediation, comparing European and US approaches that, while they share a concern for the influence of digital platforms, diverge in their cultural premises and regulatory visions.

1. The algocracy in the era of digital information

According to Aneesh (2006, 2009), algocracy, a term originally connected to the organization of the workplace, describes a networked digital environment in which informational power is increasingly exercised by algorithms that enable certain modes of interaction and organization while inhibiting others. Danaher later expanded this notion, defining algocracy as 'a system in which algorithms are used to collect, compare and organize the data by which decisions are made thereby shaping the ways in which individuals interact with information and with one another within governance systems' (2016, pp. 2–3). Algorithms are conceived as precise, executable sequences of actions designed to solve specific problems, and are characterized by the finiteness of the steps, their generality in referring to and solvinga class of problems, and the unambiguity and repeatability of the nexus between data and results (Sartor, 2022, pp. 96–97). In this sense, they function as tools of governance and as forms of 'politics by other means' (Latour, 1988, p. 142), embodying the technocratic logic of digital power. Consequently, in a society where information is widely shared and mediated through data correlations and algorithmic selection, it paradoxically entails inhabiting a 'black-box society' (Pasquale, 2015), in which the boundaries between state and market increasingly blur.

In this regard, a relevant critical issue is represented by the economic exploitation of digital data, often obtained through mere exchanges on the Web, but in the absence of the fully informed and conscious consent of the stakeholders (Faini, 2019, p. 316; Rodotà, 2014, pp. 27–32), an exploitation which is set up by a small number of public and private operators able to control the wealth of information, and exercising, in an opaque way, an epistemic monopoly (Orrù, 2021, p. 205) and an authority equal, if not superior, to that of national governments in guiding the opinions and actions of citizens (Zambonelli, 2020, p. 13). In this way, a private and self-regulatory power, which takes on the characteristics of factual sovereignty, puts in place political mechanisms of dubious legitimacy that introduce unprecedented forms of surveillance and discrimination (Rodotà, 2012, pp. 394–395) that reflect on the very future of democracy (Faini, 2019, p. 63) – unknowns that are made even more serious by their lack of spatial circumscription or corresponding legal regulation (Casonato,

2019b, p. 178). Furthermore, a lot of disinformation can be found on the Web, fuelled by fake news (Ziccardi, 2019, p. 187) and often also supported by national media and institutional profiles, which are aimed at obtaining a direct, albeit virtual, relationship with citizens (Ziccardi, 2019, p. 23): this, in the abstract, could present a considerable possibility for information and participation, but unfortunately it frequently resolves in the discrediting of divergent opinions and leads to distracting attention from issues of general relevance (Habermas, 2023, p. 69). The viral amplification of messages lowers the level of public discussion and political debate (Habermas, 2023, pp. 64, 113–114), generating a gradual overlap between public and private. In fact, 'real-time digital democracy is a *democracy of presence*: it turns the smartphone into a *mobile parliament* that debates continuously and everywhere […] It accelerates the degeneration of the public sphere because it tirelessly publicizes the private sphere' (Han, 2023, pp. 35–36; emphasis original). These dynamics have significant implications for the protection of individual rights (Ziccardi, 2019, p. 37), as seen from the proliferation of fake profiles, trolls, spam, viruses and chatbots that generate algorithmic communication flows mimicking natural conversation (Ziccardi, 2019, pp. 70–71, 188).

Equally concerning is the phenomenon of reverse censorship, which drowns out unwelcome or minoritarian information in an overabundance of content, fabricating artificial consensus around specific viewpoints. As algorithms gain prominence in managing online information, private actors – digital platforms and internet service providers – have gradually assumed functions traditionally held by public authorities. In this context, the algocracy reaches its full expression in the infrastructural power of platforms that shape the digital environments where knowledge is produced and circulated, performing a quasi-normative role that deeply influences rights and democratic deliberation. This underscores the need for a flexible, multi-stakeholder regulatory framework in which self-regulation complements public oversight (Faini, 2019, p. 411; Stradella, 2020, p. 80), ensuring that decisions of general interest are subject to political deliberation and the realization of democratic values.

2. The challenges of surveillance capitalism for democratic systems

The growing concentration of knowledge, driven by the supranational dimension of the Web and by a regulatory framework that remains largely reactive to digital transformation (Faini, 2022), threatens substantive equality (De Minico, 2019, p. 113). At the same time, public authorities' use of private digital data further risks enabling mass surveillance systems through partnerships with major technology companies (Faini, 2019, pp. 183–187), undermining the openness of democratic societies (Hayes, 2012, pp. 167–175). Meanwhile, the increasing privatization of the Web has consolidated the power of a few 'landowners of knowledge' (Orefice, 2018,

p. 158), laying the foundations for 'surveillance capitalism' (Zuboff, 2019), which produces 'equivalence without equality' (Zuboff, 2019, p. 394) and reduces individual freedom to the lowest common denominator of the virtual market. This allows a pervasive economic logic that goes so far as to predict and modify individual actions, including political and electoral behaviour, altering the most basic democratic principles and the meaning of popular sovereignty (Barberis, 2020; O'Neil, 2017; Zuboff, 2019).

This phenomenon supports the algorithmic selection of online content based on previously expressed preferences, and represents a threat to democracy by reducing meaningful discussion in the public sphere, fostering polarization, making individuals more vulnerable to censorship, propaganda or even self-propaganda (Pariser, 2011; Sunstein, 2017) and fuelling the rise of populism (Habermas, 2017). In this way, 'microtargeting' weakens the democratic process and the rule of law (Han, 2023, p. 27), 'because voters are not educated on a party's political program. Instead, they are shown manipulative advertising and not infrequently fake news tailored to their psychodrama' (Han, 2023, p. 28). This refers to an interpretation of reality to which the virality of its dissemination lends the qualification of authenticity (Ziccardi, 2019, p. 52). The emergence of multiple 'filter bubbles' (Pariser, 2011) illustrates how algorithmic recommendation systems tend to confine users within cultural and ideological boundaries, exposing them mainly to content that reinforces their pre-existing beliefs and producing increasingly personalized outputs. By restricting exposure to diverse viewpoints, filter bubbles also risk diminishing creativity, intuition and learning, while weakening social capital (Pariser, 2011) and ultimately eroding the potential of a pluralist public sphere. In this sense, they foster self-referential communication that blurs the line between the private and public domains, giving rise to competition among semi-public spaces (Habermas, 2023, pp. 61–67).

These dynamics are also reflected in the notion of echo chambers (Sunstein, 2017), where individuals tend to seek political information consistent with their own views and engage primarily with like-minded people (Han, 2023, pp. 43–45). Such mechanisms undermine public deliberation and civil debate (Sunstein, 2017), while revealing the growing asymmetry of knowledge between information producers and users (Casonato, 2019a, pp. 714–715). As a result, already shared information gains even greater visibility, despite the digital realm's vast potential to disseminate diverse data and news. At the same time, users risk being absorbed into 'digital swarms' (Baumann, 2010, p. 97) that amplify herd-effect behaviours (Ziccardi, 2019, p. 217). Thus, critically reflecting on algocratic power and on the identification of the responsibility of the political system to prevent these phenomena, significant questions about freedom of expression, pluralism and informational fairness emerge, placing algorithms, in their function as content filters capable of nurturing crystallized thinking that limits personal and collective choice (Zambonelli, 2020, pp. 118–121) at the centre of the

discussion, in opposition to the rational justification of democratic decisions (Habermas, 2002, pp. 33–35; 2023, pp. 65–69).

3. The right of freedom of expression on the Web

3.1. The American normative and judicial approach

The concentration of technological and informational power in the hands of major platforms has turned algocracy, which Danaher (2016) sees as a 'threat' toward democratic systems, into one of the most pervasive forms of digital governance, compelling a serious consideration of how different legal systems respond to these dynamics. Since algorithmic power acts as a new form of private regulation over collective experience, the legal response inevitably mirrors each system's conception of freedom, responsibility and rights protection. In this sense, the European and US approaches, though both aware of the political and social impact of digital platforms, rest on distinct cultural and philosophical foundations, leading to divergent ways of balancing technological innovation with democratic safeguards.

The United States' legal and judicial approach to online information emphasizes freedom of expression and limited legal liability for digital platforms. In the US, the legal approach to online information in fact rests on two basic pillars: the First Amendment to the Constitution and Section 230 of the Communications Decency Act, the first rule introduced by Congress, in 1996, to regulate the role of internet service providers. These regulatory instruments have shaped a digital environment characterized by considerable freedom of expression and a distinctive role for online platforms, which enjoy very limited legal liability: indeed, the First Amendment very broadly protects freedom of speech and of the press and has been interpreted by case law as also applying to online expression. This means that, in general, the state cannot censor or restrict content published on the Web unless it falls into very narrow categories, such as incitement to violence or defamation, and up to the point of bordering on hypotheses of child pornography. This protection has fostered the development of an open and pluralistic digital environment, although not without problems related to the circulation of disinformation or hate content. Rounding out the picture is Section 230 of the Communications Decency Act, a provision with a crucial impact on the way the internet has developed which states that interactive online service providers are not to be held liable for user-generated content. In addition to this type of immunity, Section 230 also grants platforms the right to freely moderate content, filtering or removing it, without losing their legal protection, thus becoming true players in the information mediation process. In fact, although originally conceived as neutral intermediaries, platforms actually operate by their own criteria in the selection, promotion or removal of content, often through opaque algorithms and internal policies that are not always clear and effective, with a profound impact

on public opinion and the visibility of content. Consequently, in recent years the role of platforms has been in the centre of lively political debate, starting from Section 230, in the assessment of whether these digital actors, which are private in nature, can implement content moderation choices that are not allowed to public authorities, which are directly bound by the First Amendment (Bassini, 2019, pp. 49–52). On this point, on the one hand conservatives accuse platforms of restricting freedom of expression, especially regarding content that is right-wing or contrary to mainstream culture; on the other, progressives criticize the lack of control over harmful content, such as health misinformation or hate speech. In this conflict of positions, both sides have raised the issue of possible reform of Section 230, but so far no concrete proposal has been able to take firm hold.

In American juridical decisions, there are some significant rulings; in this regard, a landmark case is *Trump v. Twitter*, in which the (then-former) US president was banned from the platform after the assault by some of his supporters on Capitol Hill on 6 January 2021. The case reignited the debate over the power of platforms to silence even prominent political figures, and highlighted how private regulation of content can conflict with the public perception of free speech (Judgment of the US Supreme Court, 2022). Another significant judgment is *Gonzalez v. Google*, considered by the US Supreme Court in 2023: in this case, family members of a victim of a terrorist attack accused YouTube, owned by Google, of 'amplifying' radical content through its algorithms. The case raised profound questions about the degree to which platforms are responsible not only for what they host, but for how they convey information; since the Court avoided a ruling that would fundamentally change the legal framework, the debate remains open (Judgment of the US Supreme Court, 2023; Fabiano, 2024, p. 98).

Very interesting, since it presents elements of distance from previous rulings, is the judgment of the Supreme Court in *Moody, Attorney General of Florida, et al. v. Netchoice, LLC, DBA Netchoice, et al.* (Judgment of the US Supreme Court, 2024) on the freedom of expression and guarantees offered by the First Amendment, a ruling that considers not so much, as previously, aspects of the non-responsibility of digital platforms, but rather their activity of moderating content which may fall within the free manifestation of thought (Fabiano, 2024, p. 89). This decision in fact represents the first case in which content moderation is seen as a right of the managers of online platforms, based on the guarantee of the First Amendment (Bassini et al., 2024; Mantovani, 2024). From this very recent perspective that examines the activity of content moderation, therefore, the focus is shifted from the guarantee for private subjects from possible government interference to considering any limitations of thought that can be carried out by other private subjects (Fabiano, 2024, p. 90). Therefore, in this specific case, the Opinion of the Court on the merits concerns the freedom of expression of the manager of the digital platform, and refers to the state laws of Texas and Florida which, in addition to providing limits to the activity of content moderation,

also required that the provider had justified its decisions for content censorship. The Opinion of the Court – taking into account that the lower courts had not correctly carried out the social challenge control, that is, they had correctly evaluated the contested regulation in all its possible implications, considering instead only the position of the major providers (Fabiano, 2024, pp. 103–104) – therefore highlighted how the government cannot interfere in the expression of private thought, since the purpose of Section 230 is the protection of freedom of thought from public influence (Fabiano, 2024, p. 95). In this way, the Supreme Court decision of 1 July 2024 could be a first step toward ever-increasing freedom of expression on social networks; all the positive aspects of this must be considered, but so also must be the critical issues represented by the possible manipulation and conditioning of collective thought, which on this point increases the already notable distance from the European approach to these issues (Fabiano, 2023; Fabiano, 2024, p. 100; Pollicino, 2023).

Overall, the US legal approach has fostered an online ecosystem strongly oriented toward freedom of expression and technological innovation, but it has left large 'grey areas' regarding the accountability of digital platforms, a principle carefully considered instead by both the 2018 European General Data Protection Regulation (GDPR, 2016, Art. 24) and the Digital Services Act (DSA, 2022, Arts. 4–20). The American perspective to date does not seem to consider the gradual transformation of the role of online platforms from mere infrastructure providers into powerful information brokers, raising urgent questions about the future of internet regulation, digital democracy and the balance between freedom and responsibility. While this approach has fostered an open, dynamic and innovative internet, it has also contributed to the spread of disinformation, online hate speech and extreme content, with minimal regulatory intervention by the state.

3.2. The European regulatory and jurisprudential approach

The European context detaches itself from the American approach, being characterized by constitutional provisions aimed at broadly, but not absolutely, protecting the freedom of manifestation of thought (Abbondante, 2017, pp. 56–59). This principle, is in fact, balanced with other values and rights of equal importance, such as human dignity, the right to identity and personal image, privacy and personal data protection. Second, even in the first European regulatory orientation, the online service provider, as of the dictate of the now-dated E-Commerce Directive no. 31/2000, the online service provider is under no obligation to monitor or check in advance the content of posts and comments entered by users, or to actively search for facts or circumstances indicating illegal activities, except where the provider takes an active role in conveying the information; this latter aspect outlines the distinction between content moderation activities, the figures of a mere transmission provider, cache provider and host provider, and the related legal responsibility (Directive 2000/31/EC, Arts. 12–14). This approach is outlined in the famous *Google Spain* judgment (Judg-

ment of the CJEU, 2014), where the CJEU held that a search engine operator acts as a 'controller' of personal data when indexing third-party web pages, recognized its active role in affecting fundamental rights and confirmed its responsibility to evaluate and, where appropriate, remove links upon delisting requests.

The gradual expansion of the functions of online service providers over the years, in some cases to trace attitudes proper to public authorities (Bassini, 2019, p. 55), has, however, prompted an increasingly broad interpretation of the role and responsibilities referable to such entities. Even the European Union has developed a direction aimed at increasing the accountability of online providers beyond the provisions of Directive 2000/31/EC, as witnessed by the EU Commission's 2017 Guidelines about the obligation to monitor information transmitted or stored by online service providers. This increases the providers' aggravating their burden by enshrining the principles of 'take-down', imposed by the need for Member States to provide detailed regulation of the process leading to the effective and timely removal of illicit content, and 'stay-down', preventing the reappearance of illicit content similar to that already subject to take-down.

In the regulatory field, the European Union is also moving in a different direction, aiming to balance freedom of expression with the protection of human dignity, the rights of consumers and democracy. In fact, for greater protection of the delicate balance between freedom of expression and the guarantee of the correctness of online information, the European Union has in recent years introduced several key pieces of legislation: here, it is worth mentioning the GDPR, which establishes protective rights for users over their personal data and imposes stringent obligations on digital platforms on transparency, individual consent and the processing of user data. Also relevant is the 2023 Digital Markets Act, which regulates online information 'gatekeepers' in order to prevent anticompetitive practices, including restrictions on combining personal data from different sources, a set of obligations to allow users to install applications from third-party platforms, prohibitions on bundling services, and a prohibition on promoting one's own services under certain conditions, which, in this case, cannot be offered in a more favourable way in rankings. Furthermore, the Data Governance Act encourages the reuse of some public data and the creation in the European marketplace of a data-sharing space.

A particular mention should also be made of the 2022 Digital Services Act, which came into effect in 2024, inspired by the principle that 'what is unlawful *offline* must also be unlawful *online*' (Council of the European Union, 2021) and introducing rigorous accountability obligations for digital platforms, primarily for very large online platforms. To tackle illegal content and online misinformation, the Digital Services Act establishes clear obligations for digital service providers, proportional to the size and risks of the platforms. These include measures to quickly counter illegal content while respecting fundamental rights such as freedom of expression and data protection (Arts. 12–14, 17–19). Marketplaces must enhance the tracking and monitoring

of traders to ensure product safety and must conduct random checks to prevent the reappearance of illegal content (Arts. 22–25). The Act also prohibits deceptive practices, including 'dark patterns' designed to manipulate users' choices, and restricts certain forms of targeted advertising, such as those aimed at minors or based on sensitive data (Arts. 24, 27). Very large online platforms and search engines – defined as those with at least 45 million monthly users – face additional obligations imposed by the Commission to prevent systemic risks, including the spread of illegal content, impacts on fundamental rights, interference in electoral processes, gender-based violence and mental health issues, and must undergo independent audits (Arts. 26–34). Furthermore, platforms must provide users with the option to opt out of algorithmic recommendations based on profiling and allow authorized authorities and researchers access to the platform's data and algorithms, while avoiding anticompetitive practices (Arts. 29–31, 33–34). As can be noticed, the DSA calls for the transparency, as far as possible, of algorithms, effective content moderation procedures and the introduction of systems for the rapid removal of illegal content, promoting systemic risk assessment with reference to disinformation, online violence and the protection of minors.

Measures such as the DSA or GDPR are particularly interesting in this field of study because they can foster significant regulatory influence. While the DSA regulates platform governance within the EU, its implications also connect to the broader 'Brussels effect' (Bradford, 2020), through which EU rules shape global practices as multinational companies adapt to European requirements to access the EU market. Although this dynamic traditionally underscores the contrast between the EU's rights-based model and the more market-driven US approach, it also fosters convergence, as firms often adopt EU-compliant practices globally, contributing to greater alignment between European and US frameworks.

Some interesting aspects can also be pointed out on the jurisprudential level, such as the 2019 *Glawischnig-Piesczek v. Facebook Ireland* ruling, regarding a liability case for defamatory content, specifically concerning an Austrian policy that had called for the removal of offensive content posted on Facebook. In this regard, the CJEU ruled that a platform can be obliged to remove or block offending content, even equivalent or identical content, globally, clearly increasing the liability of platforms in dealing with defamatory content (Judgment of the CJEU, 2019). The role of platforms in the sharing of copyrighted content was also addressed by the ruling in *YouTube and Cyando*, which concerns certain cases related to the unauthorized sharing of copyrighted material on YouTube and Uploaded. In this regard, the CJEU ruled that platforms are not automatically liable, but they may be liable if they do not act quickly after reporting, with the reinforcement of the concept of liability contingent on knowledge and inaction (Judgment of the CJEU, 2011). Finally, on the problematic relationship between data protection and market competition, mention should be made of the *Meta Platforms Ireland v. Bundeskartellamt* ruling of 2023, which fol-

lowed the German competition authority's challenge to Meta's use of data collected without explicit consent: the CJEU has, therefore, confirmed that antitrust authority can intervene in privacy issues, thereby enhancing consumer protection on multiple fronts, such as privacy, competition and transparency (Judgment of the CJEU, 2023). As can be seen, in the European approach, major online platforms can no longer operate as neutral subjects but are considered actors with specific powers and responsibilities, and have to ensure a secure and transparent digital environment that complies with fundamental rights.

Conclusions

The issue of freedom of expression in the digital world cannot be confined to commercial considerations, as it involves the delicate balance between freedom and responsibility, the role of AI, concrete expressions of freedom of thought and the serious risk of thought manipulation by digital tools (Fabiano, 2024, p. 107; Manganelli, 2023), which have the potential to influence the democratic stability of state of law (Fabiano, 2024, p. 101). Consequently, in the absence of spatial boundaries that can frame virtual interactions, it becomes essential to harmonize diverse world views and their corresponding regulatory frameworks concerning the role and responsibilities of major online operators, while ensuring that technology remains anchored to the universal dimension of fundamental rights (Rodotà, 2014, pp. 58–59). In this regard, cooperation between the EU and the United States could be grounded in a mix of regulatory instruments, shared standards, institutional dialogue and joint research initiatives, capable of reconciling the European vision, centred on individual rights and the protection of the public interest, with the US approach, more focused on market dynamics and innovation.

As algorithms must reflect human values and ethical principles, even at the cost of efficiency (O'Neil, 2017, pp. 294–299), it becomes essential to adopt an approach that is 'ethical by design' and that incorporates fairness, transparency and accountability throughout the entire development process. This means using representative data, creating explainable and modular systems and ensuring human oversight through specific checkpoints. These efforts must be supported by auditing mechanisms, the traceability of decisions, and tools to remedy unfair outcomes, alongside active user and public participation to align technologies with shared social values. Ultimately, ensuring that algorithms operate in line with fundamental rights and the public good requires the integration of ethics, technology and governance, while the promotion of digital literacy and lifelong learning is essential to cultivate awareness and responsibility in the face of potential algorithmic threats to democracy.

REFERENCES

Abbondante, F. (2017). Il ruolo dei social network nella lotta all'hate speech: un'analisi comparata fra l'esperienza statunitense e quella europea. *Informatica e diritto*, *43*(1/2), 41–68.

Amato Mangiameli, A. C. (2019). Algoritmi e big data. Dalla carta sulla robotica. *Rivista di filosofia del diritto/ Journal of Legal Philosophy*, *8*(1), 107–124.

Amato Mangiameli, A. C., & Campagnoli, M. N. (2020). *Strategie digitali. #diritto_educazione_tecnologie*. Giappichelli.

Aneesh, A. (2006). *Virtual migration: The programming of globalization*. Duke University Press.

Aneesh, A. (2009). Global labor: Algocratic modes of organization. *Sociological Theory*, *27*(4), 347–370.

Barberis, M. (2020). *Come internet sta uccidendo la democrazia. Populismo digitale*. Chiarelettere.

Bassini, M. (2019). La cassazione e il simulacro del provider attivo: Mala tempora currunt. *MediaLaws – Rivista di Diritto dei Media*, *2*, 248–257.

Bassini, M., Finocchiaro, G., & Pollicino, O. (2024, 7 October). Il 1 emendamento USA tutela le piattaforme e dà loro un ruolo editoriale. *Il Sole 24 Ore*. https://www.ilsole24ore.com/art/il-primo-emendamento-usa-tutela-piattaforme-e-da-loro-ruolo-editoriale-AFmB0MiC

Baumann, Z. (2010). *Consumo, dunque sono*. Laterza.

Bradford, A. (2020). *The Brussels effect: How the European Union rules the world*. Oxford University Press.

Casadei, T., & Pietropaoli, S. (2021). *Diritto e tecnologie informatiche. Questioni di informatica giuridica, prospettive istituzionali, sfide sociali*. Wolters Kluwer.

Casonato, C. (2019a). Costituzione e intelligenza artificiale: un'agenda per il prossimo futuro. *BioLaw Journal/ Rivista di BioDiritto*, *25*, 711–724.

Casonato, C. (2019b). Potenzialità e sfide dell'intelligenza artificiale. *BioLaw Journal/Rivista di BioDiritto*, *1*, 177–182.

Council of the European Union, What is illegal offline should be illegal online: Council agrees position on the Digital Services Act, 25 November 2021, https://www.consilium.europa.eu/en/press/press-releases/2021/11/25/what-is-illegal-offline-should-be-illegal-online-council-agrees-on-position-on-the-digital-services-act/

Danaher, J. (2016). The threat of algocracy: Reality, resistance and accommodation. *Philosophy & Technology*, *29*, 245–268.

De Minico, G. (2019). Big Data e la debole resistenza delle categorie giuridiche. Privacy e lex mercatoria. *Politica del diritto*, *1*, 89–115.

De Tullio, M. F. (2016). La privacy e i big data verso una dimensione costituzionale collettiva. *Politica del diritto*, *4*, 637–696.

Durante, M. (2019). *Potere computazionale. L'impatto delle ICT su diritto, società, sapere*. Meltemi.

European Parliament and Council. (2000). Directive 2000 no. 31 on Certain Legal Aspects of Information Society Services, in Particular Electronic Commerce, in the Internal Market. https://eur-lex.europa.eu/eli/dir/2000/31/oj/eng

European Parliament and Council. (2022, 14 September). Regulation 2022/1925 on Contestable and Fair Markets in the Digital Sector and Amending Directives (EU) 2019/1937

and (EU) 2020/1828 (Digital Markets Act). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32022R1925

European Parliament and Council. (2022, 19 October). Regulation 2022/2065 on a Single Market for Digital Services and Amending Directive 2000/31/EC (Digital Services Act). https://eur-lex.europa.eu/eli/reg/2022/2065/oj/eng

Fabiano, L. (2023). Le potenzialità manipolative della democrazia digitale fra interessi pubblici e poteri privati. *Diritto dell'informazione e dell'informatica*, *4–5*, 597–643.

Fabiano, L. (2024). Content moderation e free speech clause: il controverso rapporto fra libertà e responsabilità delle piattaforme digitali nella più recente giurisprudenza della Corte suprema federale USA. *Federalismi. Rivista di Diritto Pubblico, Italiano, Comparato, Europeo*, *27*, 88–107.

Faini, F. (2019). *Data society. Governo dei dati e tutela dei diritti nell'era digitale*. Giuffrè.

Faini, F. (2022, 8 June). *Principi etici e giuridici per la tecnologia*. Media2000. https://www.media2000.it/fernanda-faini-giurista-digitale-principi-etici-e-giuridici-per-la-tecnologia/

Floridi, L. (2012). *La rivoluzione dell'informazione*. Codice.

Floridi, L. (2017). *La quarta rivoluzione. Come l'infosfera sta trasformando il mondo*. Raffaello Cortina.

Foucault, M. (1975). *Sorvegliare e punire. Nascita della prigione*. Einaudi.

Habermas, J. (2002). *Il futuro della natura umana. I rischi di una genetica liberale*. Einaudi.

Habermas, J. (2017). La risposta democratica al populismo di destra. *Micromega*, *2*, 4–24.

Habermas, J. (2023). *Nuovo mutamento della sfera pubblica e politica deliberativa*. Raffaello Cortina.

Han, B.-C. (2022). *Le non-cose. Come abbiamo smesso di vivere il reale*. Einaudi.

Han, B.-C. (2023). Infocrazia. Le nostre vite manipolate dalla rete. Giulio Einaudi Editore.

Hayes, B. (2012). The surveillance-industrial complex. In *Routledge handbook of surveillance studies* (pp. 167–175). Routledge.

Jasanoff, S. (2004). *States of knowledge: The co-production of science and the social order*. Routledge.

Judgment of the CJEU of 13 May 2014 on the case of *Google Spain, S. L., Google Inc. v. Agencia Española de Protección de Datos and Mario Costeja González*. https://op.europa.eu/en/publication-detail/-/publication/1df672d5–05b4–11e4–831f-01aa75ed71a1/language-en

Judgment of the CJEU of 3 October 2019 on the case of *Glawischnig Piesczek v. Facebook Ireland*. https://curia.europa.eu/juris/document/document.jsf?text=&docid=218621&pageIndex=0&doclang=IT&mode=req&dir=&occ=first&part=1&cid=49929

Judgment of the CJEU of 22 June 2021 on the case of *YouTube and Cyando*. https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:62018CJ0682

Judgment of the CJEU of 4 July 2023 on the case of *Meta Platforms Ireland v. Bundeskartellamt*. https://curia.europa.eu/juris/document/document.jsf;jsessionid=F3DD0CA874FF40844471F-2F6AC22FD50?text=&docid=275125&pageIndex=0&doclang=IT&mode=req&dir=&occ=-first&part=1&cid=97875

Judgment of the US Supreme Court of 5 June 2022 on the case of *Trump v. Twitter.* https://www.govinfo.gov/app/details/USCOURTS-cand-3_21-cv-08378/context

Judgment of the US Supreme Court of 18 May 2023 on the case of *Gonzalez v. Google* no. 21–1333. https://www.supremecourt.gov/opinions/22pdf/21–1333_6j7a.pdf

Judgment of the US Supreme Court of 1 July 2024 on the case of *Moody, Attorney General of Florida, et al. v. Netchoice, LLC, DBA Netchoice, et al.*, no. 22–277. https://www.supremecourt.gov/opinions/23pdf/22–277_d18f.pdf

Latour, B. (1988). The politics of explanation: An alternative. In S. Woolgar (Ed.), *Knowledge and reflexivity: New frontiers in the sociology of knowledge* (pp. 155–176). Sage.

Manganelli, A. (2023). Piattaforme digitali e social network fra pluralità degli ordinamenti, pluralismo informatico e potere di mercato. *Giurisprudenza Costituzionale*, *2*, 883–904.

Mantovani, E. (2024, 18 July). Piattaforme digitali: l'attività di selezione dei contenuti è protected speech. La Corte Suprema USA limita gli interventi di regolazione statale nel settore digitale. *Diritti Comparati*. https://www.dirittocomparati.it/piattaforme-digitali-lattivita-di-selezione-dei-contenuti-e-protected-speech-la-corte-suprema-usa-limita-gli-interventi-di-regolazione-statale-nel-settore-digitale/

Monti, M. (2019, 15 October). *La corte di giustizia, la direttiva e-commerce e il controllo contenutistico online: le implicazioni della decisione C 18–18 sul discorso pubblico online e sul ruolo di Facebook*. MediaLaws. https://www.medialaws.eu/la-corte-di-giustizia-la-direttiva-e-commerce-e-il-controllo-contenutistico-online-le-implicazioni-della-decisione-c-18–18-sul-discorso-pubblico-online-e-sul-ruolo-di-facebook/

O'Neil, C. (2017). *Armi di distruzione matematica. Come i Big Data aumentano la disuguaglianza e minacciano la democrazia*. Bompiani.

Orefice, M. (2018). *I Big Data e gli effetti su privacy, trasparenza e iniziativa economica*. Aracne.

Orrù, E. (2021). Verso un nuovo Panottico? La sorveglianza digitale. In T. Casadei & S. Pietropaoli (Eds.), *Diritto e tecnologie informatiche. Questioni di informatica giuridica, prospettive istituzionali, sfide sociali* (pp. 203–216). Wolters Kluwer.

Palazzani, L. (2020). *Tecnologie dell'informazione e intelligenza artificiale*. Studium.

Pariser, E. (2011). *The filter bubble: How the new personalized web is changing what we read and how we think*. Penguin.

Pasquale, F. (2015). The Black Box Society: The Secret Algorithms That Control Money and Information. Harvard University Press.

Perri, P. (2020). *Sorveglianza elettronica, diritti fondamentali ed evoluzione tecnologica*. Giuffrè.

Pollicino, O. (2023). Di cosa parliamo quando parliamo di costituzionalismo digitale? *Quaderni costituzionali*, *3*, 569–594.

Rifkin, J. (2001). *L'era dell'accesso. La rivoluzione della new economy*. Mondadori.

Rodotà, S. (2012). *Il diritto di avere diritti*. Laterza.

Rodotà, S. (2014). *Il mondo nella rete: quali i diritti, quali i vincoli*. Laterza.

Sartor, G. (2022). *L'informatica giuridica e le tecnologie dell'informazione*. Giappichelli.

Stradella, E. (2020). Stereotipi e discriminazioni: dall'intelligenza umana all'intelligenza artificiale. *Consulta Online*, 1–10. https://giurcost.org/contents/giurcost//LIBERAMICORUM/stradella_scrittiCostanzo.pdf

Sunstein, C. R. (2017). *#republic: Divided democracy in the age of social media*. Princeton University Press.

Talia, D. (2018). *La società calcolabile e i big data. Algoritmi e persone nel mondo digitale*. Feltrinelli.

Thurman, N. (2011). Making 'The daily me': Technology, economics and habit in the mainstream assimilation of personalized news. *Journalism: Theory, Practice & Criticism*, *12*(4), 395–415.

Thurman, N., & Schifferes, S. (2012). The future of personalization at news websites: Lessons from a longitudinal study. *Journalism Studies*, *13*(5–6), 775–790.

Zambonelli, F. (2020). *Algocrazia. Il governo degli algoritmi e dell'intelligenza artificiale*. Scienza Express.

Ziccardi, G. (2019). *Tecnologie per il potere. Come usare i social network in politica*. Raffaello Cortina.

Zuboff, S. (2019). *Il capitalismo della sorveglianza. Il futuro dell'umanità nell'era dei nuovi poteri*. Luiss University Press.

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

sciendo

DOI: 10.15290/bsp.2026.31.01.03

Received: 06.08.2025
Accepted: 23.09.2025

Viktoria Mazur
Tallinn University of Technology, Estonia
viktoria.mazur@taltech.ee
ORCID ID: 0009–0003–2212–1057

David Ramiro Troitiño
Tallinn University of Technology, Estonia
david.troitino@taltech.ee
ORCID ID: 0000–0002–0542–5724

Unequal by Design? Reclaiming Digital Access as a Fundamental Right in the EU

Abstract: This article explores the EU's evolving approach to digital inclusion, focusing on how current policies and legal frameworks address the needs of vulnerable groups. Despite ambitious targets under the Digital Decade Policy Programme 2030, large disparities persist along lines of age, education, geography, and migration status. Drawing on recent Eurostat data, legal analysis, and case studies from Member States, the article identifies key structural and design-based barriers that prevent meaningful participation in the digital society. It argues that digital inclusion must go beyond infrastructure and skills training to become a guaranteed right, integrated into enforceable legal standards. The analysis highlights both progress and critical gaps in EU policy, such as a lack of binding subgroup targets and uneven accessibility provisions. The article concludes with concrete recommendations for turning digital inclusion from an aspirational value into a legal, operational, and measurable component of European citizenship.

Keywords: digital inclusion, EU policy, vulnerable groups, digital divide

Introduction

The digital transformation of European society is advancing rapidly, with growing reliance on online services, e-governance, and digital tools. Within this landscape, e-governance plays a crucial role: it not only improves administrative efficiency by re-

ducing bureaucracy, but it also fosters European integration, transparency, and trust (de la Guardia, 2005). However, it is vital to ensure that all citizens can access and benefit from these digital services.

Despite the EU's ambitious digital goals addressed in the Digital Decade Policy Programme 2030, significant differences remain in citizens' access to digital services and their ability to use them effectively – a phenomenon commonly referred to as the digital divide. The latest Eurostat data shows that this divide persists across geography, age, education, and socio-economic background within the European Union. As of 2024, 94% of EU households had access to the internet, but this figure hides important differences: while urban households such as cities are connected at fairly high levels, cities, suburbs, and rural areas still have lower rates of access, and in some countries internet access in rural areas falls dramatically compared to cities (e.g. Greece and Bulgaria have 15 percentage points' difference) (Eurostat, 2024a). Furthermore, although 85.9% of the EU population aged 16–74 reported daily internet use, this rate drops to just 80.3% in rural communities and to 59.2% for people aged 65–75 (Eurostat, 2023b). Alarmingly, 6% of Europeans in this age group had never used the internet at all in 2023, and in some regions, such as Greece, this figure exceeded 17%. Nevertheless, in 2024 this figure dropped to 14%, which shows a positive trend (Eurostat, 2024a). Digital skills remain another critical area of concern. While 56% of Europeans aged 16–74 have at least basic digital skills (Eurostat, 2024b), this statistic illustrates a huge gap among older adults: only around 29% of those aged 65–74 have such skills (Eurostat, 2023a). Educational attainment also plays a decisive role: 80% of people with tertiary and higher education have basic digital skills, compared to 34% of people with little or no formal education. Gender gaps persist as well, with men slightly ahead of women in digital competence across most age groups, although young women (16–24) currently outperform their male counterparts (72% v. 68%), while women aged 65–74 lag behind by more than 10% (23% v. 34%) (Eurostat, 2025).

These figures show that despite high levels of internet penetration and political commitments to creating a digitally inclusive Europe, substantial barriers remain for many citizens, particularly in rural areas and among older populations, women, and those with low levels of education, not to mention disabled people and migrants, who have additional obstacles in accessing digital services. Addressing these differences is not only a matter of social equity; it is also important for the broader project of European integration. According to the neo-functionalist approach, digital integration generates spillover effects that contribute to deeper integration (Kerikmäe et al., 2019; Troitiño, 2022). However, without targeted efforts to bridge the digital divide, these effects risk entrenching new inequalities within the European Union.

This article examines how current EU policies and initiatives respond to the needs of vulnerable groups in the context of digital transformation, and focuses on whether these efforts effectively promote equality and inclusion across demographic, geographic, and socio-economic divides. The analysis draws on official EU policy

documents, the latest European statistics, and relevant academic literature. The article is structured as follows: the first section provides an overview of the EU's strategic framework and key programmes aimed at promoting digital inclusion. The second section analyses how these initiatives address the specific needs of vulnerable groups, including older people, rural populations, migrants, and people with low levels of education or digital skills. The third section discusses the main challenges and barriers to implementation, such as uneven coordination between Member States and gaps in digital accessibility. Finally, the article highlights what current policies mean in practice and points to ways in which the EU could make digital inclusion more effective and more accessible to all.

1. Bridging the gap: The EU's response to the digital divide

The European Union has recognised the urgency of combating the digital divide and has addressed this challenge through a progressively structured legal and policy framework. Ensuring that all citizens, regardless of age, gender, or background, can meaningfully participate in the digital society is increasingly seen as a prerequisite for the success of Europe's digital transformation. Strengthening digital literacy, closing gender gaps in digital access, and supporting older adults and other at-risk groups are now essential components of inclusive policymaking. This understanding is reflected in several key EU initiatives that aim to promote digital inclusion and ensure that no one is left behind in Europe's digital transformation (Peeters et al., 2025). This journey began with the Digital Compass 2030, which defined four key dimensions of the digital transformation: digital skills, digital infrastructures, business digitalisation, and public services, thus laying the groundwork for a cohesive and inclusive digital Europe.

The Digital Compass sets what the EU aims to achieve by 2030. The Digital Decade Policy Programme 2030 states how it will be achieved by turning those goals into enforceable laws and structured governance – national plans, regular reporting, monitoring, stakeholder involvement, and shared projects – all anchored in EU-level accountability. The Digital Decade programme guides these goals into achievable targets and introduces concrete governance tools, which include an annual State of the Digital Decade report, national strategic roadmaps, and a 'traffic light' monitoring system to evaluate Member States' progress (European Parliament and Council, 2022, articles 5–6). One of the programme's core objectives is that at least 80% of those aged 16–74 have at least basic digital skills by 2030. The policy programme also underscores the importance of bridging the digital divide, with a special focus on older citizens, individuals with lower educational attainment, and residents of rural areas (Negreiro, 2015). If digital strategies are not carefully and thoughtfully designed, they can actually make existing inequalities worse rather than better (Djatmiko et al., 2025).

The Digital Compass sets out a vision for Europe's digital future. While it outlines broad ambitions, its language remains somewhat general when it comes to addressing the unique barriers faced by vulnerable groups. It has been pointed out that this lack of detailed mechanisms or dedicated funding streams limits the potential impact on digital inclusion (Ayata, 2024; Ferretti, 2022). To help operationalise these goals, the EU has launched the Digital Skills and Jobs Platform, which offers resources, training opportunities, and community networks to improve digital competences across Europe. Importantly, the platform includes targeted initiatives for groups with lower levels of digital skills, such as older adults and jobseekers (Rek, 2024; Rūse, 2014). However, participation rates among the most marginalised groups remain uneven, and further outreach efforts appear necessary (Costa, 2023; Djatmiko et al., 2025; Giovanola, 2023; Hamuľák, 2016). In addition to skills, two other factors, language and geographical access, have an impact on who can benefit from digital services.

The European Union first acknowledged this issue in the 2017 European Parliament report 'Linguistic Equality in the Digital Age', which warned that the dominance of English and a few mainstream languages in the digital sphere was exacerbating the exclusion of speakers of minority and regional languages with limited resources. The report laid the foundation for the Human Language Project and the European Language Equality (ELE) initiative. Developed as part of a large-scale EU research consortium (2021–2023), the ELE aims to achieve digital linguistic equality by 2030 by supporting automated translation, language technologies, and inclusive content design. Although the ELE is not legally binding, it has shaped research agendas and funding priorities at EU level, directly strengthening digital inclusion across language barriers – especially for communities historically underrepresented online.

In parallel, the EU Geo-Blocking Regulation (Regulation (EU) 2018/302) eliminates unjustified segmentation of the digital marketplace based on nationality, residence, or location. It prohibits practices that restrict access to websites, prices, or services based on where a person lives in the EU, a critical step towards a more cohesive digital single market. By allowing users from Member States to access the same content, e-commerce opportunities, and services regardless of location, the Regulation addresses territorial forms of digital exclusion. Together, these measures strengthen the EU's efforts to create an accessible and inclusive digital environment, not only through infrastructure or legal rights, but also through concrete mechanisms that remove hidden barriers.

Another important milestone is the European Declaration on Digital Rights and Principles for the Digital Decade (2022), which sets out values that should guide Europe's digital transition. The declaration highlights accessibility, inclusiveness, and citizen empowerment, reaffirming that digital services should be designed for all Europeans, regardless of age, gender, ability, or socio-economic background, and putting people at the centre of the digital transformation. While the declaration is not legally binding, it provides a normative reference point for Member States.

A legally binding step in this direction is the European Accessibility Act (EAA), Directive (EU) 2019/882, which was adopted in 2019 and fully applied in all EU Member States by 28 June 2025. The Act establishes harmonised accessibility requirements for a wide range of digital products and services, including ATMs, smartphones, e-books, banking services, and e-commerce platforms. Its core aim is to ensure that people with disabilities, as well as older adults and other users with functional limitations, can independently access and use essential digital tools. Ensuring compatibility with assistive technologies (such as screen readers, voice recognition, or switch controls), enforcing minimum usability standards based on POUR principles (perceivable, operable, understandable, and robust through WCAG/EN 301 549[1]), and requiring provision of accessible formats (e.g. alt-text, captions, large print, braille), the EAA addresses one of the key dimensions of the digital divide: interface exclusion. Unlike general policy declarations, this law imposes legal obligations on businesses and service providers across the single market, with enforcement mechanisms at the national level. Although primarily framed around disability rights, the EAA's provisions benefit a broader range of vulnerable users, helping to ensure that the transition to digital-first service delivery does not leave behind those with physical, sensory, or cognitive limitations.

The EU is also preparing to strengthen its legal tools with the upcoming Digital Fairness Act, expected by 2026. This proposed legislation will introduce clear rules to make digital spaces more transparent and accessible. For example, it will ban deceptive designs, known as 'dark patterns', that push people to click things they do not fully understand or agree with. These tricks can be especially confusing for older people, those with lower digital skills, or users who face language or cognitive barriers. The law will also require websites and platforms to present information in a clear and understandable way, so that everyone, regardless of age, education, or background, can use digital services more confidently and independently. This matters because even when people have internet access and devices, poor interface design can quietly shut them out. Many users struggle to complete tasks, feel frustrated, or give up entirely when faced with confusing layouts or overwhelming information (Eurostat, 2024; Zac et al., 2025, p. 5). Others may become dependent on family members or carers to help them navigate online services – which undermines their autonomy and privacy. These are not technical problems but design ones, yet they create real exclusion. Traditional policies aimed at expanding infrastructure or access do not fix this hidden UX barrier. By focusing on how digital tools are actually designed and experienced by users, the Digital Fairness Act will aim to remove everyday obstacles that quietly exclude the most vulnerable.

1 It is a European accessibility standard that outlines technical accessibility criteria for IT and ICT products and services. This standard provides detailed guidance for ensuring that various technologies are accessible to people with disabilities.

In addition to strategic frameworks, the European Union provides substantial financial support to drive digital transformation and inclusion. Several major funding programmes channel investments into projects aimed at reducing the digital divide and fostering equitable access to digital opportunities. The Digital Europe Programme (2021–2027), with a total budget of over EUR 8.1 billion, is one of the core instruments supporting Europe's digital objectives. In the period 2025–2027 alone, approximately EUR 1.3 billion is allocated to enhancing digital skills, promoting artificial intelligence, and strengthening cybersecurity capacities (European Commission, 2025a). Complementing this is Horizon Europe R&I funding – around EUR 1.4 billion in 2025 – which invests in deep-tech innovations and high-potential start-ups via the European Innovation Council (European Commission, 2024b; Reuters, 2024). Targeted support for social inclusion is provided through the European Social Fund Plus (ESF+), which invests in education, training, and digital skills development for vulnerable groups. Numerous projects funded under ESF+ focus on equipping vulnerable populations such as older adults, migrants, and low-income communities with essential digital competences (Maatsch, 2024; Mokrá, 2023). Moreover, Erasmus+ supports digital transformation in education. The European Student Card Initiative, for example, aims to achieve 95% digital learning agreements by 2025, facilitating greater accessibility and mobility for students across Europe (European Commission, 2025a).

Beyond these programmes are large-scale investment initiatives such as InvestAI, which aims to mobilise EUR 200 billion for AI development. If managed inclusively, this can enhance public services (e.g. in healthcare or education) and create more accessible, user-friendly digital tools, especially when paired with ethical AI and human-centred design. However, without safeguards, it could also widen gaps, hence the need to channel parts of this investment into inclusive AI solutions. The Global Gateway strategy allocates EUR 300 billion for infrastructure, including digital connectivity, which is critical for closing the connectivity gap, particularly in rural, remote, or underserved regions. Reliable infrastructure is the baseline requirement for digital access; without it, skills training or digital services are irrelevant (European Commission, 2025a).

The importance of combining legal frameworks with user-centred implementation is supported by recent empirical research. Morte-Nadal and Esteban-Navarro (2025) highlight that without enforceable design standards, mechanisms to gather user feedback, and legal accountability, e-government strategies often fall short, especially in providing tailored, accessible services to older adults, low-income individuals, and those with limited education. Their study recommends embedding binding co-creation processes, simplified hybrid (digital and in-person) service models, and transparency obligations, elements that the Digital Fairness Act aims to deliver. Together, these investments reflect a multi-layered approach to addressing Europe's digital divide: by improving infrastructure, fostering innovation, and supporting digital

skills development among vulnerable groups. Yet, as subsequent analysis will show, ensuring that these resources effectively reach those most at risk of exclusion remains an ongoing challenge.

2. Challenges in addressing the needs of vulnerable groups

2.1. Persistent inequalities in digital inclusion

Addressing the needs of vulnerable groups remains one of the most pressing challenges in the European Union's digital transformation (Gomes & Dias, 2025; Outeda, 2024). Despite ambitious policy frameworks and considerable investment, the reality on the ground continues to show deep inequalities in access to digital services and skills. The groups most affected include older adults, people with lower levels of education, women, residents of rural areas, migrants, and economically disadvantaged communities. These populations often face multiple and overlapping barriers to digital inclusion, ranging from lack of access to devices and internet infrastructure to low levels of digital literacy and systemic institutional obstacles. Statistical evidence highlights the persistence of these disparities. While younger, urban, and well-educated Europeans generally report high levels of internet use and digital competence, older adults and rural residents remain significantly underrepresented online. In Estonia, for example – often cited as a leader in e-governance – only around 70% of people aged 65–74 report daily internet use, compared to over 95% among people aged 16–64 (Statistics Estonia, 2024). Similar gaps persist across the Union, particularly in southern and eastern Member States.

2.2. Language, design, and other barriers to digital inclusion

EU-level initiatives such as the Digital Skills and Jobs Platform and projects funded by the European Commission seek to address these disparities by promoting digital skills development among disadvantaged groups. However, while these programmes provide valuable resources and training opportunities, their reach and impact remain uneven. Participation by the most marginalised populations often depends on the strength of local outreach, the availability of targeted support, and the adaptability of the training to the specific needs of different groups. In practice, many vulnerable citizens still have difficulty using digital services due to several barriers. Older people often lack confidence in using digital tools or fear making mistakes, leading to avoidance (Reid et al., 2024; Vaportzis et al., 2017). People with disabilities often encounter poorly designed websites or apps that are incompatible with assistive technologies such as screen readers or alternative input methods (Droutsas et al., 2024). The problem is not that making websites or apps accessible is impossible; it is that accessibility is often not considered during the design stage, or it is added too late, after everything is already built (Shah, 2023). This makes many digital services

hard or even impossible to use for people with disabilities, even if they have assistive tools like screen readers. Women, especially those from low-income or minority families, may face increased challenges due to unequal access to education, lower levels of exposure to digital technologies, and household responsibilities that limit time to develop skills (Perifanou & Economides, 2020). People with lower levels of formal education are more likely to have difficulty navigating complex interfaces or understanding the technical language used on digital platforms (Rivera Pastor et al., 2017). These challenges are often compounded by a lack of plain language instructions or multilingual content, further alienating users from different backgrounds.

In addition to skills and interface design, access to digital content can also be restricted by territorial and linguistic barriers. One example is the unintended effect of the EU Geo-Blocking Regulation, which was originally designed to ensure fair access to online goods and services within Member States. However, as recent analyses show, it does not protect access to audiovisual content, a category in which linguistic minorities often suffer the most. As a result, speakers of regional or minority languages may be disproportionately excluded from culturally significant content or unable to access services in their native language, especially across borders (Röggla, 2025). Such exclusions create a digital environment in which not all EU citizens can participate equally, despite formal principles of non-discrimination. Addressing this issue will require expanding existing legal protections or developing new ones that explicitly take linguistic diversity into account in the digital sphere.

In addition to the above-mentioned challenges, legal and administrative barriers continue to limit access to certain groups. New legislative proposals such as the Digital Identity Regulation and the European Health Data Space (EHDS) show how digital tools are becoming gateways to essential services. The Digital Identity Regulation will allow all EU residents to use a secure European Digital Identity Wallet to access services such as banking, e-signatures, e-government portals, and healthcare, using a single, interoperable digital ID. While the wallet is seen as a key tool for promoting digital inclusion, its implementation has raised some concerns about fairness for migrants and refugees, who may lack the necessary documentation or legal status to register (Cheesman, 2022; Dullaert et al., 2024; Tabassum et al., 2025). Without tailored measures, these groups risk losing access to these services – ironically, leaving those who would benefit most from digital inclusion on the margins. Currently, registration for the wallet is dependent on the provision of official proof of identity and citizenship-issued credentials, such as a passport, national identity card, driving licence, or proof of residence accepted by a Member State wallet provider (European Commission, 2025b). As several Member States still require full legal residence status, many migrants and refugees, especially those with pending documents or who have temporary protection status, are effectively excluded from the system. Although some pilot projects are testing alternative credentials or migrant-friendly pathways,

these have not yet been integrated into the mainstream framework, creating significant gaps in access and reinforcing existing inequalities.

Similarly, the EHDS interface aims to make personal health data more accessible and shareable across borders. For many patients, especially those with chronic conditions, disabilities, or cross-border mobility, this can provide greater care and empowerment. However, if digital health systems are not designed with accessibility in mind, they risk excluding people who lack digital skills, face cognitive barriers, or cannot afford private technologies. Older people, low-income patients, and people with disabilities are particularly at risk of being left behind in the transition to digital health. Without clear guarantees, what is meant as a right of access can become another form of exclusion. These cases highlight a broader point: laws that promote innovation and cross-border interoperability must be designed with accessibility and equity at their core.

2.3. National strategies and local best practices

Fortunately, certain Member States provide examples of effective approaches to address the digital divide. For instance, Estonia actively supports digital inclusion as part of its e-governance. The government provides free digital literacy courses for older people and access to public services on user-friendly platforms, including support through libraries and community centres (European Union Agency for Fundamental Rights (FRA), 2023). Additionally, as part of the national Digital Decade strategy, Estonia is developing the Digimentor system to train and support older users. These approaches demonstrate the effectiveness of individual support and blended learning (online and offline). Similarly, the Digital Inclusion project by Česko.Digital in the Czech Republic focuses on increasing digital literacy among social workers – and through them, among vulnerable groups: the elderly, the unemployed, and people with disabilities. According to the Digital Skills and Jobs Platform, the survey and interviews covered about 794 responses, and the project developed a training module aimed at more than 10,000 social workers, thereby training their clients. Elsewhere in the EU, Poland has launched the Erasmus+ pilot project Adult Social Inclusion in the Digital Environment (ASIDE), which equips social educators and volunteers with the skills needed to support older people, families with children, and disadvantaged communities. By facilitating collaboration between grassroots organisations, ASIDE offers a promising model for scaling up citizen-focused digital literacy initiatives (Sánchez-García et al., 2021). However, such best practices are far from universal across the EU. In many countries, public investment in digital inclusion remains fragmented, and national digital strategies do not always prioritise reaching the most excluded groups.

2.4. Institutional trust and media literacy

An additional layer of complexity arises from the different levels of public trust in digital governance. In highly digitalised countries such as Estonia and Denmark, e-government enjoys strong public support. According to the UN E-government Study 2024, both countries are among the world leaders in the scope and quality of their online government services. In parallel, a recent OECD trust survey (OECD, 2024) found that 44% of Danes report high or moderately high trust in their national government, compared to 38% of Estonians – a figure close to the OECD average. In contrast, Member States with lower levels of digital adoption often show greater scepticism about government-led digital initiatives. This gap reflects broader patterns of institutional trust rather than digital service quality per se, and highlights the importance of aligning technical progress with citizen engagement and transparency. Such caution typically stems from concerns about data privacy or surveillance, or worries that digital systems could exacerbate inequality. This discrepancy highlights why improving access alone is not enough; citizens must also have media and digital literacy, which enables them to navigate and critically evaluate digital tools and services. The Audiovisual Media Services Directive obliges Member States to integrate media literacy education into national curricula and report on progress every three years. However, implementation has been inconsistent, largely due to differences in political commitment across countries, resulting in uneven awareness-raising campaigns, educational programmes, and support infrastructures (Laaninen, 2025). Overall, while the EU has made significant progress in recognising and addressing the digital divide, many vulnerable groups still face persistent structural barriers to fully participating in Europe's digital society. These barriers are not simply technical or economic in nature; they increasingly intersect with issues of fundamental rights and legal powers.

2.5. Recognising the digital divide: A legal perspective

Recent cases concerning digital exclusion illustrate once again how access to digital technologies has become inseparable from the enjoyment of fundamental rights in various areas of life. Vulnerable groups are not simply asking for improved services or amenities; they are seeking recognition that full participation in modern European society increasingly depends on the ability to access and use digital tools. Digital inclusion is not only a matter of access to infrastructure, but of being institutionally included in the systems that shape access to rights, information, and opportunity (Stein et al., 2022, p. 2). Denying such access may amount to a violation of fundamental rights protected by European and international law.

Several recent judgments by the European Court of Human Rights (ECtHR) and national courts have made this point clear. In *Jankovskis v. Lithuania* (2017), the ECtHR found a violation of Article 10 of the European Convention on Human Rights after a prisoner was denied access to educational material online. The Court stressed that internet access is increasingly important for the enjoyment of rights such as edu-

cation and information, and that states must take measures to mitigate digital exclusion. Importantly, the Court clarified that the right to information in the digital age cannot be interpreted narrowly or arbitrarily restricted, especially when access to education is at stake. While the court's decision acknowledged that certain restrictions may be justified in closed institutions, it ruled that general bans without individual assessment or proportionate justification do not meet democratic standards. It sets an important precedent for digital rights within prisons and emphasises that contextual restrictions must meet genuine necessity and proportionality requirements, especially when education and reintegration are at stake (Judgment of the ECtHR, 2017, paragraphs 54, 59–62). The case marked a major turning point in the recognition of digital access as an integral part of the enjoyment of fundamental rights.

A recent legal case in Slovakia (Poradňa pre občianske a ľudské práva – Center for Civil and Human Rights, 2025) illustrates the complexities of addressing digital exclusion through anti-discrimination law. A Roma student brought a claim against the state, arguing that she had been denied access to digital learning during the COVID-19 pandemic due to a lack of internet and digital equipment. Although the District Court initially ruled in her favour, the decision was overturned by the Court of Appeal, and upon retrial, the case was dismissed in January 2025. While the final judgment did not establish digital exclusion as a form of discrimination, the case sparked public debate on the structural barriers faced by marginalised groups in accessing education, particularly in the context of digital transitions.

These cases show that vulnerable groups are making a clear and powerful statement: digital access has become fundamental to realising many of the rights and opportunities required for equal citizenship. Their demands go beyond technical fixes; they demand reliable and affordable access to infrastructure and devices, inclusive and accessible design of digital services, and legal recognition of digital access as an integral part of social and civil rights. Equally important, they seek meaningful participation in the design and governance of digital public services to ensure that their experiences and needs are not overlooked but actively shape the systems designed to serve them.

3. Policy implications and future directions

The evidence provided in this study confirms that European frameworks have created a common vocabulary for digital inclusion, but they have not yet produced significant common results. Measurable gaps persist based on geography, age, gender, education, disability, and migration status. Unless the next policy cycle moves from ambitious promises to achievable standards, today's inequalities risk becoming tomorrow's structural divisions.

Pan-European targets such as '80% of adults should have at least basic digital skills by 2030' are a helpful benchmark, but they miss out the fact that all Member

States have very different starting points. In 2023, less than 30% of Europeans aged 65–74 had basic skills, compared to 80% of persons with a higher education (Eurostat, 2024b). Therefore a young university graduate living in a city is not starting from the same place as an older woman in a rural village or a newly arrived migrant. While the EU's Digital Decade programme sets clear targets for the population as a whole, Member States are not required to break these down by group; there are no binding obligations, for example, to ensure that a certain percentage of older people or low-income migrants achieve digital literacy benchmarks by a certain year. National roadmaps exist but vary in scope and ambition, and many vulnerable groups are still left behind. If digital inclusion is really of the essence, EU policies need to become more specific. Member States should be asked to set clear national targets for the most at-risk groups and show how they plan to reach them. These targets should come with deadlines and funding, just like the EU's economic goals do.

Soft law instruments like the Declaration of Digital Rights help to set shared values and influence the direction of policy, but they lack legal force – they cannot force governments or companies to follow through. By contrast, the EAA is legally binding; it shows how hard law can close a critical gap when digital services and devices are designed in ways that exclude people with disabilities or older users. Starting from June 2025, products like ATMs, e-readers, e-commerce apps, and banking apps will not be allowed on the EU market unless they meet the EAA's accessibility requirements. The same approach – making accessibility mandatory – should be applied to other major digital laws that are currently under development or revision, including the upcoming Digital Identity Regulation, the European Health Data Space, and the Digital Fairness Act. If accessibility is built in as a default legal requirement across all these frameworks, it would ensure that digital tools are usable by everyone from the start, not just adapted afterwards.

Even when the infrastructure is in place, confusing interfaces, dark patterns, or English-only content silently exclude vulnerable users. If the forthcoming Digital Fairness Act is to truly promote inclusion, it must go beyond vague obligations and directly address the interface barriers that keep such users out. The Act should therefore:

- ban manipulative consent flows and other dark patterns that disproportionately confuse older adults and users with limited digital or linguistic skills;
- require public-sector websites and major platforms to comply with EU-wide usability standards, including the Web Content Accessibility Guidelines (WCAG 2.2) and plain-language norms;
- mandate regular usability testing with representative samples of vulnerable users, such as seniors, persons with disabilities, and minority-language speakers, to ensure that services are not only legally accessible but practically usable.

These provisions would help shift the EU's approach from symbolic inclusion to actual usability, ensuring that digital access is meaningful for all citizens, not just those already equipped to navigate it. But regulation alone is not enough. Member States should be encouraged, and where necessary obliged, to fund targeted digital inclusion programmes, especially those that have proven effective in reaching marginalised groups. For example, the Czech Digital Inclusion initiative, which trains social workers to transfer digital skills to vulnerable clients, shows how capacity building at the grassroots level can enhance the impact of EU-level goals. National strategies should actively support such community-led efforts, focusing not only on technical infrastructure, but also on support systems for people who enable digital participation in real life, prioritising people's needs, behaviours, and experiences.

Combining digital and media literacy has been shown to improve user engagement, critical thinking, and confidence, particularly among vulnerable groups (IDMO, 2023; IRIS CoE, 2024). A strategic target could be to allocate at least 25% of ESF+ funds to digital skills development in curricula that integrate both technical and critical literacy, in partnership with public service broadcasters and local media. While the Digital Europe and Horizon Europe programmes allocate significant resources to digital transformation, only a small proportion is allocated to accessible design or underserved regions. To reduce regional inequalities, at least 10% of the Digital Europe capacity-building budget could be allocated to projects targeting the lowest-performing Digital Economy and Society Index (DESI) quartile. The EU could use its multi-country project mechanism under the Digital Europe programme to jointly develop open-source tools, such as voice interfaces in minority languages, that could be reused in smaller Member States, thereby reducing duplication and increasing linguistic inclusiveness.

Finally, recent court cases also show that courts are prepared to regard digital exclusion as a form of discrimination. To build on this trend, the Commission should issue interpretative guidance, clarifying how digital contexts fall within the scope of the Race Equality and Goods and Services directives, and support strategic litigation to test these principles in practice. This means making clear that non-discrimination applies both online and offline: digital services should not be designed to systematically disadvantage people on the basis of language, ethnicity, gender, or other protected characteristics. Access to essential services such as e-government, healthcare, or banking should not depend on having the latest device, a fast connection, or knowledge of the dominant language. If a digital service effectively excludes certain groups, those affected should be able to complain and seek remedies, just as if they were denied a service in the physical world. Incorporating digital inclusion into the Charter will help transform fundamental rights into enforceable protections in the digital age.

Building trust is the final, overarching challenge. Surveys show that low trust in digital public services correlates with low usage, especially when users feel they do not control their data or understand how it is used. Transparent, accountable systems can

bridge this gap. Public dashboards should monitor service performance, security or privacy incidents, and results of accessibility audits, in real time. AI systems used in welfare, policing, or migration must be licensed with accessible summaries, including minority-language versions, and local 'digital ombudsmen' offices should mediate complaints, offer human support, and build confidence among marginalised users.

Together, these measures would transform the EU's current patchwork of pilots and strategies into a coherent, rights-based digital inclusion policy. They align infrastructure with human-centred design, turn soft commitments into enforceable law, and embed user feedback in governance. Digital inclusion should not remain a policy aspiration; it must be recognised and enforced as a fundamental right, embedded in the EU's legal and political framework alongside other core citizenship rights.

Conclusion

The digital divide is not a passing technical problem but a structural fault line that determines who can participate in modern European society. This article shows that while the EU has made significant progress in creating a common framework for digital inclusion, the lived experiences of many citizens, especially older people, migrants, rural residents, and those with low levels of education, still reflect deep and persistent inequalities. Closing these gaps will require more than just setting targets or funding pilot projects; it will require treating digital inclusion as a matter of justice and enforceable rights. This means embedding accessibility and usability into all digital laws and public services, funding programmes that create real support systems for vulnerable users, and holding national strategies accountable for reaching the most vulnerable. As digital access becomes a gateway to fundamental rights – from education and healthcare to legal protection and civic participation – the EU must move beyond symbolic inclusion to legal guarantees. If digital tools become the new infrastructure of citizenship, the right to access and use them must be protected with the same seriousness as other civil and social rights.

REFERENCES

Ayata, Z. (2024). European Union contracts in digital environments. In D. Ramiro Troitiño (Ed.), *E-governance in the European Union: Strategies, tools, and implementation* (pp. 173–185). Springer Nature Switzerland.

Cheesman, M. (2022). Digital wallets and migration policy: A critical intersection. *The Dialogue on Tech and Migration, DoT.Mig.* https://www.bosch-stiftung.de/sites/default/files/publications/pdf/2022–06/Digital%20Wallets%20and%20Migration%20Policy.pdf

Costa, M. I. (2023). The legal concept of discrimination by association: Where does it fit into the digital era? *UNIO–EU Law Journal*, *9*(1), 16–28.

de la Guardia, R. M. (2005). La política europea de España después de su integración en las Comunidades. *Cuadernos europeos de Deusto*, *32*, 61–84.

Djatmiko, G. H., Sinaga, O., & Pawirosumarto, S. (2025). Digital transformation and social inclusion in public services: A qualitative analysis of e-government adoption for marginalized communities in sustainable governance. *Sustainability*, *17*(7), 2908. https://doi.org/10.3390/su17072908

Droutsas, N., Spyridonis, F., Daylamani-Zad, D., & Ghinea, G. (2024). Web accessibility barriers and their cross-disability impact in esystems: A scoping review. *Computer Standards & Interfaces*, *92*, 103923. https://doi.org/10.1016/j.csi.2024.103923

Dullaert, I., Weitzberg, K., Schoemaker, E., & Martin, A. (2024). *The European Digital Identity Wallet: Why it matters and to whom*. Caribou Digital Publishing.

European Commission. (2021, 9 March). *2030 Digital Compass: The European way for the Digital Decade* (COM(2021) 118 final).

European Commission. (2024a). *Bridging the digital divide: 95% of learning agreements to be fully digital by 2025*. https://erasmus-plus.ec.europa.eu/news/bridging-the-digital-divide-95-of-learning-agreements-to-be-fully-digital-by-2025

European Commission. (2024b). *The second Horizon Europe strategic plan 2025–2027*. https://ec.europa.eu/commission/presscorner/detail/en/ip_25_2612

European Commission. (2025a). *2025 State of the Digital Decade package*. https://digital-strategy.ec.europa.eu

European Commission. (2025b). *European Commission adopts new round of EU Digital Identity Wallet implementing regulations*. https://ec.europa.eu/digital-building-blocks/sites/spaces/EUDIGITALIDENTITYWALLET/pages/909706465/New+round+of+EU+Digital+Identity+Wallet+implementing+regulations+adopted

European Parliament and Council. (2018, 28 February). Regulation (EU) 2018/302 on Addressing Unjustified Geo-Blocking and Other Forms of Discrimination Based on Customers' Nationality, Place of Residence or Place of Establishment within the Internal Market.

European Parliament and Council. (2019, 17 April). Directive (EU) 2019/882 on the Accessibility Requirements for Products and Services (European Accessibility Act).

European Parliament and Council. (2022, 14 December). Decision (EU) 2022/2481 on a Policy Programme 'Path to the Digital Decade' (O. J. L 323, 19.12.2022, pp. 4–26). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32022D2481

European Union Agency for Fundamental Rights (FRA). (2023). *Fundamental rights of older people: Ensuring access to public services in digital societies*. https://fra.europa.eu/en/publication/2023/fundamental-rights-older-people-digital-societies

Eurostat. (2023a). *Digital skills in 2023: Impact of education and age*. https://ec.europa.eu/eurostat/web/products-eurostat-news/w/ddn-20240222–1#:~:text=In%202023%2C%2055%25%20of%20people,individuals'%20levels%20of%20digital%20skills.

Eurostat. (2023b). *Digital society statistics at regional level*. https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Digital_society_statistics_at_regional_level

Eurostat. (2024a). *Digital economy and society statistics – households and individuals*. https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Digital_economy_and_society_statistics_-_households_and_individuals

Eurostat. (2024b). *Skills for the digital age*. https://ec.europa.eu/eurostat/statistics-explained/index.php?oldid=627685

Eurostat. (2025). *Towards Digital Decade targets for Europe*. https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Towards_Digital_Decade_targets_for_Europe

Ferretti, F. (2022). A single European data space and data act for the digital single market: On datafication and the viability of a PSD2-like access regime for the platform economy. *European Journal of Legal Studies*, *14*, 173–218.

Giovanola, B. (2023). Justice, emotions, socially disruptive technologies. *Critical Review of International Social and Political Philosophy*, *26*(1), 104–119.

Gomes, A., & Dias, J. G. (2025). Digital divide in the European Union: A typology of EU citizens. *Social Indicators Research*, *176*, 149–172.

Hamuľák, O. (2016). *National sovereignty in the European Union: View from the Czech perspective*. Springer.

IDMO. (2023). *Digital Media Literacy Gaps and Needs*. Italian Digital Media Observatory. https://www.idmo.it/wp-content/uploads/2023/12/IDMO-Digital-Media-Literacy-Gaps-and-Needs_EN_final_compressed.pdf

IRIS CoE (Council of Europe). (2024). *Media literacy and the empowerment of users* (IRIS 2024–2). https://rm.coe.int/iris-2024–2-media-literacy/1680b06196

Judgment of the District Court of Prešov of 6 November 2023 on the case of *Rozsudok v. Mene Slovenskej Republiky*, no. 18C 96/2022–254.

Judgment of the European Court of Human Rights of 17 January 2017 on the case of *Jankovskis v. Lithuania*, application no. 21575/08.

Kerikmäe, T., Ramiro Troitiño, D., & Shumilo, O. (2019). An idol or an ideal? A case study of Estonian e-governance: Public perceptions, myths and misbeliefs. *Acta Baltica Historiae et Philosophiae Scientiarum*, *7*(1), 71–80.

Laaninen, T. (2025). Media literacy: Fostering a key civic skill in a digital information environment. *European Parliamentary Research Service*. https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2025)772886

Maatsch, A. (2024). Parliamentary adjustment during a crisis: Interplay of digitalization and domestic context factors. *Internet of Things*, *27*, 101316.

Mokrá, L. (2023). Digitally sovereign individuals: The right to disconnect as a new challenge for European legislation in the context of building the EU digital market. In D. Ramiro Troitiño, T. Kerikmäe, & O. Hamuľák (Eds.), *Digital development of the European Union: An interdisciplinary perspective* (pp. 189–197). Springer International Publishing.

Morte-Nadal, T., & Esteban-Navarro, M. A. (2025). Recommendations for digital inclusion in the use of European digital public services. *Humanities and Social Sciences Communications*, *12*(1), 1–15.

Negreiro, M. (2015). Bridging the digital divide in the EU. *European Parliamentary Research Service*. https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2015)573884

OECD. (2024). *OECD Survey on Drivers of Trust in Public Institutions – 2024 results: Country notes (Denmark and Estonia)*. https://www.oecd.org/governance/trust-in-government/

Outeda, C. C. (2024). The EU's AI Act: A framework for collaborative governance. *Internet of Things*, 27(3):101291.

Peeters, R., Miller, S. M., & Schuilenburg, M. (2025). Digital government inclusion: Exploring strategies for inclusive government automation. *Government Information Quarterly*, *42*(2), 1–11. https://doi.org/10.1016/j.giq.2025.102028

Perifanou, M. A., & Economides, A. A. (2020). Gender digital divide in Europe. *International Journal of Business, Humanities and Technology*, *10*(4), 7–14.

Poradňa pre občianske a ľudské práva – Center for Civil and Human Rights. (2025). *Prešov District Court ruling in digital divide and access to education case.* https://poradna-prava.sk/en/strategic-litigation/presov-district-court-ruling-in-digital-divide-and-access-to-education-case/

Reid, M., Aleti, T., Figueiredo, B., Sheahan, J., Hjorth, L., Martin, D. M., & Buschgens, M. (2024). Factors influencing seniors' anxiety in using ICT. *Social Sciences*, *13*(9):496. https://www.mdpi.com/2076–0760/13/9/496?utm_source=researchgate.net&utm_medium=article

Rek, M. (2024). E-democracy in the EU. In D. Ramiro Troitiño (Ed.), *E-governance in the European Union: Strategies, tools, and implementation* (pp. 103–115). Springer Nature Switzerland.

Reuters. (2024, 19 April). *EU to invest $1.5 billion in region's deep tech sector.* https://www.reuters.com/technology/eu-invest-15-billion-regions-deep-tech-sector-2024–10–29/

Rivera Pastor, R., Tarín Quirós, C., Villar García, J. P., Badia Cardús, T., & Melero Nogués, M. (2017). Language equality in the digital age: Towards a Human Language Project – now! *Scientific Foresight Unit (STOA)*. https://www.europarl.europa.eu/RegData/etudes/STUD/2017/598621/EPRS_STU(2017)598621_EN.pdf

Röggla, M. (2025). Addressing the discriminatory effects of the EU geo-blocking regulation on minority groups. *Eurac Research Science Blogs*. https://doi.org/10.57708/BH0ZZX9-YSS655UM0M110IW

Rūse, I. (2014). Nordic–Baltic interaction in European Union negotiations: Taking advantage of institutionalized cooperation. *Journal of Baltic Studies*, *45*(2), 229–246.

Sánchez-García, J., Ochoa Siguencia, L., Gródek-Szostak, Z., Ochoa-Daderska, R., Kopiec, A., Szeląg-Sikora, A., Velinov, E., Sikora, J., Niemiec, M., & Akarcay, Y. (2021). Adult social inclusion in a digital environment: Digital needs for social services. *ASIDE Report II*. https://zenodo.org/records/5516367

Shah, H. (2023). Advancing web accessibility: A guide to transitioning design systems from WCAG 2.0 to WCAG 2.1. *15th International Conference on Web Services & Semantic Technology*, *15*, 233–245.

Statistics Estonia. (2024). *Daily internet use by age groups*. https://stat.ee/en/news/929-estonian-households-use-internet-social-media-increasingly-popular

Stein, V., Pentzold, C., Peter, S., & Sterly, S. (2022). Digitalization and civic participation in rural areas: A systematic review of scientific journals, 2010–2020. *Raumforschung und Raumordnung / Spatial Research and Planning*, *80*(3), 251–265. https://doi.org/10.14512/rur.112

Tabassum, S., Mathew, N., & Faklaris, C. (2025). Privacy on the move: Understanding educational migrants' social media practices through the lens of communication privacy management theory. *COMPASS '25: Proceedings of the ACM SIGCAS/SIGCHI Conference on Computing and Sustainable Societie*. https://dl.acm.org/doi/10.1145/3715335.3735453

Troitiño, D. R. (2022). The European Union facing the 21st century: The digital revolution. *TalTech Journal of European Studies*. 12(1), 60–78.

Vaportzis, E., Giatsi Clausen, M., & Gow, A. J. (2017). Older adults' perceptions of technology and barriers to interacting with tablet computers: A focus group study. *Frontiers in Psychology*, *8*(1687). https://doi.org/10.3389/fpsyg.2017.01687

Zac, A., Huang, Y., Moltke, A., Decker, C., & Ezrachi, A. (2025). Dark patterns and consumer vulnerability. *Behavioural Public Policy*, 1, 1–50. https://ora.ox.ac.uk/objects/uuid:c4f6a1b3–838a-49e7-b0d6–2f9d6b05cdb7

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

sciendo

DOI: 10.15290/bsp.2026.31.01.04

Received: 02.12.2025
Accepted: 05.03.2026

Elżbieta Kużelewska
University of Bialystok, Poland
e.kuzelewska@uwb.edu.pl
ORCID ID: 0000–0002–6092–7284

Mariusz Tomaszuk
Technical University of Warsaw, Poland
tomaszuk.m@gmail.com
ORCID ID: 0000–0003–4669–9745

Tilen Majnik
University of Ljubljana, Slovenia
Tilen.Majnik@pf.uni-lj.si
ORCID ID: 0009–0007–2367–5587

Agnieszka Piekutowska
University of Bialystok, Poland
piekutowska@uwb.edu.pl
ORCID ID: 0000–0001–7923–9484

Bruna Žuber
University of Ljubljana, Slovenia
bruna.zuber@pf.uni-lj.si
ORCID ID: 0000–0003–1137–4561

Digital Citizenship and the Right Not to Use the Internet: The European Approach[1]

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. This research was co-financed by the Slovenian Research and Innovation Agency as part of the research project V5-2383 'Theoretical and Practical Aspects of the Modernisation of Administrative Procedure in Slovenia'.

Abstract: The growing importance of the concept of digital citizenship reflects the integration of online participation, rights, and responsibilities into everyday life. European policies and initiatives increasingly emphasise digital inclusion, universal access, and the promotion of digital literacy as prerequisites for active citizenship in the digital era. At the same time, the question arises of whether individuals should also be entitled to a right *not* to use the internet without facing social, economic, or political exclusion. This article explores the European approach to digital citizenship in the context of this emerging right, highlighting tensions between policies aimed at inclusion and the freedom of individual choice. It analyses how to reconcile the promotion of digital participation with respect for the autonomy of individuals who choose to remain offline. It also argues that recognising the right not to use the internet is crucial for protecting personal freedoms and preventing forced digital dependency, while inclusive strategies should ensure that non-users are not marginalised in exercising their civic rights.

Keywords: digital citizenship, digital inclusion, right not to use the internet, civic rights, personal freedoms

Introduction

The 20th century brought with it the development of new technologies and the beginning of the digitisation of the modern world, including many aspects of social life. The 21st century, on the other hand, has seen even greater and more rapid technological development and digitisation entering virtually every aspect of human life. Nowadays, functioning without access to the internet and a smartphone in your pocket is significantly difficult, and at times downright impossible.

Technological development currently affects virtually every sphere of life – democracy, education, public services, and business – and it does not seem that this trend can be reversed. As a result, the concept of digital citizenship has emerged in the public sphere as a set of rights, obligations, competences, and civic participation that exists in or is related to the digital world. At the same time, digital citizenship has also given rise to the concept of the right not to use the internet (the right to be offline) as a privilege or right of the individual, and is sometimes understood as a new human right.

This article explores whether individuals should have the right to refrain from using the internet without facing social, economic, or political exclusion, particularly within the framework of digital citizenship. It examines the European approach to digital citizenship in the context of this emerging 'right to be offline', highlighting the tensions between policies promoting integration and the freedom of individual choice. The analysis focuses on how to encourage digital participation while respecting the autonomy of those who opt out of online activities. The article argues that recognising the right not to use the internet is essential for protecting personal freedoms and preventing forced digital dependency. At the same time, integration strategies should ensure that non-users are not marginalised in exercising their civil rights. Ultimately, it posits that digital citizenship and the right to remain offline are complementary: digital citizenship is incomplete if it does not acknowledge individuals' choice not to engage online.

The article examines the evolving concepts of digital citizenship and the emerging right to be offline within the European Union, addressing a central question: can these two seemingly opposing ideas be reconciled? The first part analyses the theoretical foundations of digital participation and individual autonomy, while the second part considers how these concepts have been implemented in European legal frameworks. Subsequent sections explore the rationale for the right not to use the internet and its place within established human rights, as well as the potential tensions or complementarities between active digital engagement and the choice to remain offline. The final section discusses policy implications, focusing on how digital inclusion can be balanced with individual freedom of choice.

The article is guided by the hypothesis that digital citizenship and the right to be offline are not necessarily contradictory and can coexist, allowing individuals to engage meaningfully in the digital sphere while retaining autonomy over their online presence. To verify this hypothesis, the study employs a dogmatic research method, drawing on European legal solutions in the field of digitalisation.

1. The conceptual framework: Digital citizenship and autonomy

When discussing the topic of digital citizenship, it is necessary to start with an understanding of the traditional concept of 'citizenship', which has been present in politics and society since ancient times. According to its etymology, the word 'citizen' comes from the word *civita*, which means 'city' in Latin. This in turn is related to the Greek word *politikós*, meaning 'a person living in a city'. In ancient Greece, the concept of citizenship was understood as the right of Greek individuals to participate in decision-making concerning the city's goals through the *ekklesia*, a practice introduced in the agora (a Greek public square used for agreeing on decisions). Greek democracy, which represented only a few people whose decisions determined the fate of the entire city (slaves, women, and craftsmen were excluded from citizenship), derives from this practice (de Moraes & de Andrade, 2015, p. 7). In modern democracy, the concept of citizenship refers to the exercise of civil, political, and social rights and duties established in fundamental state documents, in which rights and duties are interlinked to ensure the functioning of a democratic society. In this way, the interconnection of these rights and duties makes citizenship to some extent inextricably linked to the place where a person exercises them. On the one hand, being a citizen means a guarantee of all civil, political, and social rights, thus ensuring the possibility of a full life. On the other, citizens understand that these rights are not simply granted but are required, integrated, and then accepted by the law, the authorities, and the local community as a whole (de Moraes & de Andrade, 2015, p. 8).

In view of this, citizenship is seen as a relationship between people and the nation state. It is based on the concept of 'civic duty', according to which citizens are

informed about public affairs through the media and are obliged to participate in electoral processes (Bennett, 2007). Individual interests are expressed through membership of political parties and interest groups. This traditional approach to citizenship has been criticised by feminists and diversity advocates for its narrow approach to identity, expression, and participation (Vromen, 2017). Recently, new norms of citizenship have emerged based on what Vromen (2017, p. 27) calls a 'personalised politics of life', in which democratic participation is as much about electoral processes. Citizens are mobilised by specific social movements and issues, often of a global nature (e.g. climate change).

Just as citizenship itself does not have a single definition, the concept of digital citizenship is understood differently by researchers. On the one hand, it means the ability to use technology competently; interpreting and understanding digital content and assessing its credibility; creating, searching for, and communicating with appropriate tools; critical thinking about the ethical possibilities and challenges of the digital world; and making safe, responsible, and respectful choices on the internet (Isman & Güngören, 2014, p. 73). On the other hand, digital citizenship is defined as 'the right to participate in online social life' (Mossberger et al., 2007, p. 1). Early approaches to digital citizenship focused primarily on bridging the digital divide: issues of access, integration, and communication rights and freedoms were prioritised (Shelley et al., 2004; Thrane et al., 2004). However, with the proliferation of social media platforms, the issue of access has become less important, as Facebook and X, formerly Twitter have become tools for civic participation. In the digital context, citizenship is almost a given, but it involves a series of tasks or activities (decoding messages or creating a digital identity) – it is through digital activities that digital citizens are created (Isin & Ruppert, 2015).

Thus the concept of digital citizenship has evolved from one of the first definitions of it, formulated by Ribble and Bailey (2007), which focused on technological aspects and digital competences, to the definition proposed by Emejulu and McGregor (2019), which emphasises a commitment to social justice and emancipatory and alternative technologies, as well as Robles' (2009) definition, which states that a digital citizen is a natural person, whether or not a citizen of another community or state, who exercises all or part of their political or social rights via the internet, independently or through membership of a virtual community. In the same vein, Pangrazio and Sefton-Green (2021) point out that early concepts of digital citizenship concerned the right of individuals to access and participate in the internet to bridge the digital divide. Today, the relationship between citizenship and the digital world has become much more complex in the context of collective identity and social networks offering vast opportunities.

Digital citizenship goes beyond civic duties or individual responsibility; it is primarily about how digital technologies create new avenues for participation. While these technologies open up diverse online communities, engagement remains chal-

lenging for marginalised individuals who have limited or no internet access or lack digital skills (Jenkins & Carpentier, 2013). Nevertheless, digital platforms can enable meaningful forms of civic participation that have a real impact on democratic processes. A useful reference point is the definition provided by the Council of Europe (n.d.), which describes digital citizenship as the ability to participate actively, continuously, and responsibly in both online and offline communities through competent and positive use of digital technologies, whether by creating, collaborating, sharing, socialising, exploring, playing, communicating, or learning.

In essence, digital citizenship combines two dimensions. First, it involves the competences necessary for using digital technologies effectively, including learning and teaching within this framework. Second, it encompasses political and social participation at local and national levels through digital tools and social networks. This article focuses on the latter dimension, examining digital citizenship in the context of social and political engagement.

Closely related to digital citizenship is the concept of digital coercion, situations in which individuals are compelled to use digital services to perform certain tasks or participate in social and political life, regardless of their willingness or ability to do so. Digital coercion stands in clear opposition to the idea of choosing not to use digital services (Rutkowska-Tomaszewska & Gałązka, 2024). Moreover, emerging technologies, especially those based on artificial intelligence, are increasingly shaping social norms. Alongside law, these norms play a key role in structuring the social reality around us (Nieborak, 2025).

2. The European approach to digital citizenship

As this article's scope covers the issue of digital citizenship and the right to be offline in a European context, it is necessary to present this approach with particular emphasis on documents and projects prepared within the European Union. The European Commission has set several targets for Member States to achieve by 2030 in the context of digital transformation, i.e. by the end of the current decade (referred to as the Digital Decade). To this end, a specific plan has been formulated, referred to as the Path to the Digital Decade, which establishes a governance framework based on an annual cooperation mechanism with Member States to achieve the Digital Decade objectives at EU level in the areas of digital skills, digital infrastructure, and the digitisation of businesses and public services. It also aims to identify and implement large-scale digital projects involving the European Commission and Member States (European Commission, 2021a).

The entire programme is based on the so-called Digital Compass, i.e. the objectives to be achieved by the European Union and its Member States by 2030 in areas related to digitalisation. This direction was chosen mainly due to experiences related

to the COVID-19 pandemic that began in 2020, which showed that digitalisation can bring people together regardless of where they are physically located and can become a decisive factor in promoting rights and freedoms, enabling people to transcend specific territories, social positions, or social groups, and opening up new opportunities for learning, playing, working, exploring, and pursuing their ambitions. On the other hand, the crisis caused by the pandemic also revealed the weaknesses of the digital space; in particular, its increased reliance on key technologies, often originating outside the EU, highlighted its dependence on a few large technology companies, caused an influx of counterfeit products and cybertheft, and exacerbated the impact of disinformation on democratic societies (European Commission, 2021b).

In view of the above, the European Union has set four main guidelines for actions related to achieving the objectives of the Digital Decade (European Commission, 2021a): a digitally skilled society and highly qualified digital professionals;[2] secure, efficient, and sustainable digital infrastructures;[3] the digital transformation of businesses;[4] and the digitisation of public services.[5] Finally, achieving these objectives is not possible without implementing the concept of digital citizenship within the European Union, which has also been noted in programme and policy documents prepared by the European Commission.[6] The mere implementation of digital infrastructure, skills, and capabilities, and the digitisation of enterprises and public services are not sufficient to define the EU's approach to its digital future; it is also necessary to enable all Europeans to take full advantage of digital opportunities and technologies. However, as the European Commission itself points out, it is essential to ensure that the same rights that apply in the real world can be fully exercised in the virtual world (European Commission, 2021c). This means that digital citizenship cannot in any way affect the rights arising from traditional (offline) citizenship. It is worth noting that the full implementation of digital citizenship is also circumscribed by citizens' limited trust in new technologies, including on the part of public admin-

2 By 2030, at least 80% of all adults should have basic digital skills, and the EU should have 20 million ICT professionals, with more women taking up such jobs.

3 By 2030, all households in the EU should have access to gigabit connections, and all populated areas should be covered by 5G networks; the production of state-of-the-art and sustainable semiconductors in Europe should account for 20% of global production; 10,000 climate-neutral, highly secure edge nodes should be deployed in the EU; and Europe should have its first quantum computer.

4 By 2030, three-quarters of enterprises should be using cloud services, big data, and artificial intelligence; over 90% of SMEs should have at least a basic level of digital intensity; and the number of start-ups in the EU should double.

5 By 2030, all key public services should be available online; all citizens will have access to their electronic medical records, and 80% of citizens should use eID solutions.

6 The concept of digital citizenship remains closely linked to the development of e-governance (electronic public administration), which is also a key initiative of the European Commission (Nowina-Konopka, 2017).

istration officials, as well as by a shortage of IT specialists who create and implement new digital solutions in public services and support the resolution of problems related to them (Chen & Gant, 2001).

The European Commission explicitly points to the need to first and foremost safeguard the rights enshrined in the Treaty on European Union and the Treaty on the Functioning of the European Union, which contain the fundamental rights that cannot be infringed upon in any way, regardless of the purpose. Therefore the first step towards ensuring full digital citizenship is for all EU citizens to have access to the internet and the opportunity to acquire the digital skills necessary to exercise their rights under digital citizenship (European Commission, 2021c).

3. The conceptual foundations of the right not to use the internet and its role in digital citizenship

Digital technologies have become almost indispensable in contemporary life. Governments, businesses, and social services increasingly operate according to a 'digital by default' paradigm, presuming that all citizens are connected to the internet. At the same time, while efforts to promote internet access as a human right have gained momentum (De Hert & Kloza, 2012; Kaur, 2021; Lucchi, 2013; Passaglia, 2022; Pollicino, 2020; Tomalty, 2017), the other side of the coin – the right to remain offline – has only recently emerged as a subject in sustained legal and academic debate (Custers, 2019; Kloza, 2024).

The decision to live offline – for example, preferring face-to-face interaction, analogue media, and paper correspondence – may be understood as an expression of personal autonomy in shaping one's identity and social relations. Importantly, the right to privacy encompasses a 'negative' dimension: the right to be left alone, famously formulated by Warren and Brandeis (Warren & Brandeis, 1890, p. 193). as the essence of privacy. In contemporary conditions, this principle translates into the right to opt out of digital surveillance and data collection. Scholars have argued that in a world of automated data processing, remaining offline constitutes the most authentic form of exercising privacy in the context of data protection, functioning as a default setting from which any deviation requires justification (Karaboga et al., 2017, p. 43).

When public authorities or private actors move essential services exclusively online, this may result in both direct and indirect discrimination. A requirement to use the internet to access public services disproportionately affects older people, who statistically possess lower levels of digital literacy (Kużelewska et al., 2025a), as well as persons with disabilities, individuals living in rural areas with limited connectivity, and those unable to afford devices or broadband access. Although technology users or non-users do not in themselves constitute a legally protected category, there is a clear intersection with protected characteristics, since those who are digi-

tally excluded are often already socially disadvantaged. The Parliamentary Assembly of the Council of Europe recognised in 2023 that more than 40% of Europe's population lacks basic digital skills, identifying older persons, individuals with low literacy, migrants, and many persons with disabilities as 'digitally vulnerable' groups (Kużelewska et al., 2025b).

The EU's Digital Compass 2020–2030 strategy sets a target of 100% online public services by 2030. However, civil society organisations and EU institutions have pointed out a paradox: promoting fully digital public services while a significant part of the population remains unable to use them risks deepening exclusion. The proposed response combines digital skills development with the continued provision of multi-channel service delivery until full inclusion is achieved. At the same time, the language of rights is increasingly present in EU digital inclusion policy (Kużelewska et al., 2025b).

Concrete legal safeguards for offline access are already emerging. In 2021, the Walloon region of Belgium adopted a decree requiring administrative procedures to remain available in paper form at the user's request, thereby explicitly safeguarding the offline option (Kloza et al., 2025). Similarly, some Swiss cantons amended their constitutions in 2023–2024 to guarantee the 'right to live offline', ensuring that governments cannot introduce fully digital services without maintaining alternatives. Although these reforms are not yet universal, they clearly signal a broader normative shift: digitalisation must not produce discrimination or exclusion, and offline minorities require protection (SwissInfo, 2025a).

The right to remain offline can be framed as an aspect of the right to equal treatment: individuals who do not or cannot use the internet should not suffer arbitrary disadvantage. States have a positive obligation to provide alternative means of access to services and information, for example enabling an elderly pensioner to receive benefits without using digital platforms, or ensuring that rural residents without broadband access enjoy the same level of access as urban populations. From a human rights perspective, technology should be a tool for inclusion, rather than a basis for exclusion. Therefore any 'digital-only' policy must be analysed for its impact on equality and, where necessary, accompanied by offline alternatives to safeguard fundamental rights.

Explicit recognition of the right to digital exclusion would bring both practical and symbolic benefits (Kloza et al., 2025). Practically, it would establish a clear normative standard that individuals cannot be compelled to use digital technologies against their will, which would provide guidance for policymakers and prevent abuses. Symbolically, it would reaffirm that human autonomy and well-being, rather than technological efficiency, remain central to the digital transformation. As the Swiss digital-policy expert Barclay has observed, elevating such principles to constitutional status could 'bring about a change in mentality' and ensure that they are taken seriously by all actors (SwissInfo, 2025b). Some scholars further interpret

the right to be offline as a necessary counterbalance to the right to access the internet, preventing a situation where what was supposed to empower individuals (connectivity) ultimately enslaves or coerces them. Furthermore, as Rossi (2025) notes, sometimes one may wish to be offline for no particular reason – and this in itself is a legitimate exercise of freedom.

Critics of a broad right to live offline raise several concerns: (1) Practicality – could such a right hinder social progress or the effectiveness of government? Some fear that if everyone demanded the right to conduct all business on paper, it could paralyse modern systems or expose them to enormous costs. (2) Scope – would this mean that the use of all technology could be refused (what about electricity or basic information and communication technologies necessary for public safety)? (3) Potential abuse – could powerful entities (e.g. corporations) abuse this right to avoid transparency by going 'offline'? These objections can, however, be addressed through a nuanced, context-sensitive design of the right. The right to remain offline would be waivable, limited, and proportionate; it would not obstruct innovation but would require alternative solutions where justice and human dignity demand them. Importantly, it would operate primarily as a defensive right protecting individuals, rather than as a tool available to corporate actors.

In practice, implementing the right to live offline would require building a choice into the system. For government services, this means always providing an alternative mode (in person, by telephone, or on paper) for people who opt out of digital channels, in line with the 'click–call–connect' principle, whereby citizens can choose between online, telephone, or in-person access (Right to Offline Coalition, 2024). For the private sector, this would mean ensuring that essential services (banking, healthcare, utilities) offer non-digital access without additional fees or delays (and possibly introducing regulations to enforce this requirement). For employment, it would mean strengthening the right to disconnect and possibly allowing employees to request non-digital work processes where feasible. This does not mean halting digital progress: it means human-centred design that preserves individual choice.

Although no provision of international law states that 'everyone has the right not to use the internet', the current combination of laws and case law effectively recognises that people cannot be forced to digitise their lives at the expense of their fundamental rights. The right to privacy underpins this understanding, protecting personal autonomy, identity, and the intimate sphere of life from unwanted interference, which in today's context includes the choice to limit one's exposure to the digital world. The right to self-determination further reinforces personal autonomy, affirming that each person should chart their own path in relation to technology, in accordance with their values and needs, without coercion from the state or society. Freedom of expression adds a negative dimension – the freedom not to be forced to communicate in a way one does not choose – and emphasises the need for pluralism in communication channels so that offline voices are not silenced. The rights to

equality and non-discrimination ensure that technological progress does not infringe on the rights of vulnerable groups, requiring inclusive design and offline alternatives to avoid the creation of a digital underclass (Kużelewska et al., 2025a).

Against this background, it follows that digital citizenship, rooted primarily in the rights to privacy, self-determination, and freedom of expression, cannot extend beyond the scope of protection afforded by those foundational rights and freedoms. Although these rights were historically conceived to enable individuals to exercise their freedoms, chiefly by shielding them from undue state interference, contemporary legal interpretation increasingly recognises that their effective protection cannot be confined to this 'positive' dimension alone. Rather, it must also encompass the 'negative' dimension, that is, the freedom not to act, not to participate, or not to engage with a given medium or technology.

As Passaglia (2025, p. 32) observes, the jurisprudence of numerous constitutional and supreme courts confirms that fundamental rights protect both the capacity to exercise a right and the freedom to refrain from exercising it. Thus freedom of expression includes not only the right to speak but also the right to remain silent; freedom of religion entails not only the right to worship but also the right not to adhere to any faith. By analogy, if access to the internet is recognised as a right enabling individuals to participate fully in social, political, and economic life, then the decision not to access the internet must equally fall within the protected sphere of individual freedom. The fact that digital citizenship also entails positive obligations on the state to ensure access to digital infrastructure does not undermine this conclusion. On the contrary, it illustrates the hybrid nature of digital citizenship as both a social entitlement and a liberty right – one that simultaneously guarantees access to digital tools and preserves the individual's freedom to refuse them.

At the same time, as with all fundamental rights, the right (not) to use the internet is not absolute and may be subject to proportionate limitations (Jóźwicki & Szoszkiewicz, 2025, p. 108). As Kużelewska, Malinowski, and Tomaszuk (2025, p. 60) emphasise, the right to privacy under Article 8 of the European Convention on Human Rights (ECHR) is a qualified right. The case law of the European Court of Human Rights establishes that only interferences reaching a certain minimum level of seriousness engage Article 8; minor inconveniences or trivial burdens do not suffice (Judgment of the European Court of Human Rights, 2019). Where such interference is established, the proportionality test under Article 8(2) requires balancing the individual's interest in maintaining offline autonomy against legitimate public interests, such as administrative efficiency, public safety, or the prevention of fraud. In this context, courts will examine whether less intrusive measures, such as maintaining offline channels of access or providing assistance to digitally excluded individuals, could achieve the same objectives without undermining personal autonomy (Rossi, 2025).

Finally, it must be acknowledged that in exceptional circumstances, such as public health emergencies exemplified by the COVID-19 pandemic, digital tools may

temporarily become the only effective means through which certain rights can be exercised, including the rights to health, education, and freedom of assembly, while also ensuring continuity in the provision of public services and the functioning of social life (Passaglia, 2025, p. 34). Even in such contexts, however, the underlying normative principle remains unchanged: digitalisation must serve the individual, not constrain them, and any limitations on the right to remain offline must remain necessary, proportionate, and strictly justified.

4. Digital citizenship and non-users: Contradiction or complementarity?

4.1. The false dichotomy between participation and non-participation

Much of the discussion on digital citizenship focuses on ways to empower the widest possible number of people to participate actively in the digital age. This question is often examined in the context of the so-called digital divide, which separates those who possess the capabilities required to be active citizens on the internet from those who lack these capabilities (Ożóg & Puchta, 2025a, p. 13). To address the digital divide, western countries and the European Union have employed numerous measures whose scope and objectives have changed over time (Yao & Quinn, 2025, p. 2). In the early 1990s, these measures focused on providing access to information and communication technologies; however, with the expansion of internet connectivity and the consequent reduction of barriers to physical access, access itself became less problematic. Attention therefore shifted to enabling internet users to acquire adequate skills for meaningful engagement online. This led to the emergence of the concept of the second-level digital divide, defined not as a divide between those who have access and those who do not, but between those who can use the internet meaningfully and those who lack the necessary skills to do so. Lastly, efforts to reduce the digital divide focused on inequalities in the benefits derived from the internet, as such benefits are fully accessible only to internet users who are properly motivated (socially, politically, and psychologically) and who also possess the skills required to access them.

The need to combat the digital divide is inseparable from the concept of digital citizenship, which can also be understood as 'the right to participate in society online' (Pangrazio & Sefton-Green, 2021, p. 18). If a person is unable to use the internet competently, he or she is excluded from an important part of social life that is conducted online, not only in interactions with other individuals but also in interactions with governing bodies such as the state.[7] For this reason, efforts to improve digital

7 An inability to access the internet and to make effective use of new technologies thus amounts, for instance, to an inability to freely exercise the right to lead a private life in undisturbed contact with relatives and friends, the right to acquire and disseminate information and opinions, the right to participate actively in public and private life, the right to obtain appropriate healthcare, and the

accessibility and thereby reduce the digital divide are both necessary and commendable. However, when it comes to removing barriers to digital inclusion, the most common response to the side effects of universal digitalisation appears to be simply more digitalisation (Ożóg & Puchta, 2025a, p. 15), which can in turn lead to a situation where the right to use the internet becomes an obligation to do so, simply because any effective offline alternative no longer exists. It is therefore necessary to analyse the content of the right to (effectively) access the internet as a cornerstone of digital citizenship and to assess whether it also includes the right not to exercise this right and to stay offline.

In this, several international documents can be of help in understanding digital citizenship. The United Nations Human Rights Council resolution A/HRC/32/L.20, for example, emphasises that 'access to information on the internet facilitates vast opportunities for affordable and inclusive education globally, thereby being an important tool to facilitate the promotion of the right to education, while underlining the need to address digital literacy and the digital divide, as it affects the enjoyment of the right to education' (United Nations Human Rights Council, 2016, p. 2). Similarly, the Joint Declaration on Digital Rights and Principles for the Digital Decade by the European Parliament, the Council of the European Union, and the European Commission states in paragraph 6 of the preamble that 'the EU vision for digital transformation puts people at the centre, empowers individuals and fosters innovative businesses. The Decision on the "Digital Decade Policy Programme 2030" sets out the concrete digital targets based on four cardinal points (digital skills, digital infrastructures, digitalisation of businesses and of public services)' (European Parliament, Council of the European Union, & European Commission, 2023, p. 2).

Terzis (2025, p. 35) suggests that digital citizenship should not be understood solely as a personal freedom, allowing individuals to decide whether or not to exercise it. Rather, it can be conceptualised as a social right that obliges the state to take proactive measures to ensure effective internet access and to address conditions that generate various forms of digital divide. In this sense, digital citizenship imposes on the state a responsibility to provide the necessary conditions for online participation across all social groups, both dominant and marginalised, while also carrying an element of obligation for rights holders, akin to the right to education for minors.

The following section of this paper explores how digital citizenship is framed within the legal framework of the European Union and evaluates whether it is more appropriately understood as a personal freedom or as a social right that entails a duty to engage in online civic and social activities.

right to education, as well as the right to access cultural goods and services, among others (Ożóg & Puchta, 2025, p. 14).

4.2. Digital citizenship as a framework of rights, not obligations

To understand the nature of digital citizenship with regard to the right or obligation to use the internet, it should first be considered which existing rights in the European human rights protection system provide legal foundations for the right to have access to the internet and, by extension, the right not to use it (Kużelewska et al., 2025, p. 59). Perhaps the most important issue within the concept of digital citizenship is the question of privacy. Everything a person does online leaves data traces, which are analysed and used in a variety of ways, not only by other digital citizens but also by platform companies, data brokers, public institutions, and the state. Hintz, Dencik, and Wahl-Jorgensen (2019, p. 37) note that the increasingly close integration of digital technologies into everyday life means that individuals generate data traces when they connect with friends via apps, share intimate information about their personal lives through chats, vote, protest, or campaign on platforms, and conduct business interactions that enable everyday activities, from online banking to ordering food, transport, and accommodation. At the same time, this integration also means that individuals are tracked even when they are not explicitly 'using' digital tools.

All these dimensions of a person's activity are covered by the right to respect for privacy and private life under Article 8 of the ECHR. The jurisprudence of the European Court of Human Rights emphasises that personal lifestyle choices, including how individuals engage with society and technology, fall within the protective scope of private life (Kużelewska et al., 2025, p. 59). Article 8 also protects the right to self-determination, which entails individuals' freedom to decide whether and how to engage with digital tools, including the choice to refuse them, as part of an autonomous way of life. The case law of both the European Court of Human Rights and the Court of Justice of the EU, as well as EU data protection rights, reflects this emphasis on autonomy. At the same time, respect for human dignity and pluralism requires that individuals not be compelled into a uniform digital mode of living. Consequently, self-determination strengthens privacy-based arguments against excluding individuals from society solely for refusing to adopt certain technologies (Kużelewska et al., 2025, p. 61).

Another important right in the context of digital citizenship is the right to good administration, protected by Article 41 of the EU Charter of Fundamental Rights. This provision guarantees procedural entitlements, such as the right to be heard, access to one's file, and the right to a reasoned decision, and reflects broader principles of accountability, responsiveness, and openness. Susi (2025, p. 53) argues that, as digitalisation alters core human rights concepts such as legal certainty and foreseeability, the right to good administration applies both online and offline. In this context, the right not to use the internet functions as a safeguard, ensuring that public administration remains accessible offline and preventing the complete migration of administrative processes into the digital sphere.

Lastly, freedom of expression under Article 10 of the ECHR should also be mentioned in this context. It protects not only the ability to impart and receive information but also a negative dimension: the right not to be compelled to communicate or to use a particular medium. While courts have emphasised the importance of internet access for modern expression, Article 10 also safeguards the pluralism of communication channels and technological neutrality. If states make information or participation available exclusively online, they may interfere with the rights of individuals who remain offline, whether by choice or necessity. Consequently, freedom of expression can be understood to include a right to access and convey information through non-digital means, requiring states to preserve offline channels alongside digital ones (Kużelewska et al., 2025, p. 62).

Since digital citizenship, understood as the right to access and use the internet, is embedded in the aforementioned rights and freedoms, its scope of protection can be determined only by examining the scope of protection afforded by those rights. This requires assessing whether they safeguard not only their positive dimension – the ability or entitlement to access and use digital technologies – but also their negative dimension, namely the ability or right to refrain from using them. The answer to this question is decisive for determining whether digital citizenship within the EU legal order is conceived solely as an enabling right or also as one that preserves individual autonomy by protecting the choice to remain offline.

5. Policy implications: How to combine inclusion and freedom of choice

The effort to bridge the digital divide in all its forms, from a lack of physical internet access to insufficient skills and knowledge to use it effectively, is commendable and generates tangible benefits for all citizens of EU countries. According to Terzis (2025, p. 9), wide accessibility to the internet not only promotes economic development but also provides individuals with opportunities to improve their lives and the societies they inhabit through active political participation online. At the same time, however, it introduces risks, including the potential misuse of private data generated by tracing individuals' online activities, a reduction in the emphasis on offline services such as education and healthcare, which are often of higher quality than their online counterparts (e.g. telemedicine, online education), and conditions conducive to the hegemonisation of culture and dominant languages, as well as the spread of misinformation, cyberwarfare, and political manipulation (Terzis, 2025, p. 13).

Considering the nature of the right to internet access as an integral component of digital citizenship, which obliges the state to protect both its positive dimension (the right to use) and its negative dimension (the right not to use), it becomes clear that digital policies must be adequately inclusive. They should aim to bridge digital

divides and ensure internet access for marginalised groups, including the elderly, rural residents, and people with disabilities (European Parliament, Council of the European Union, & European Commission, 2023, Art. 2). At the same time, such policies must respect the human rights framework underlying digital citizenship, which safeguards not only the positive but also the negative aspects of rights and liberties. Accordingly, these policies must avoid coercion unless any restrictive measures satisfy the proportionality principle.

If the right not to use the internet is to be taken seriously as an integral component of digital citizenship, it must be reflected not only at the level of abstract rights but also in the concrete design of public services and civic participation mechanisms. Digital inclusion policies often prioritise technological efficiency and online accessibility, yet far less attention is paid, particularly outside the sphere of public administration, to the institutional safeguards required to ensure that individuals who remain offline can continue to exercise their rights on an equal footing.[8] From a legal perspective, this obligation flows directly from the human rights framework underlying digital citizenship. The right to good administration under Article 41 of the EU Charter of Fundamental Rights presupposes accessibility, fairness, and responsiveness by public authorities, regardless of the medium used. As Susi (2025, p. 54) observes, the right not to use the internet acts as a gatekeeper against the complete migration of public administration into the digital domain. Accordingly, digitalisation cannot justify lowering procedural guarantees; rather, it requires their re-articulation across both digital and non-digital environments.

In practical terms, this implies developing hybrid administrative models in which digital procedures coexist with functional offline alternatives. Such hybridity is already implicitly recognised in many national procedural frameworks, which continue to provide for oral hearings, the physical serving of documents, and parallel digital and offline channels of communication between authorities and individuals. These mechanisms serve not merely as transitional arrangements but as structural safeguards for those who cannot or choose not to engage digitally.[9] European policy documents increasingly acknowledge this need. The European Commission's eGovernment Benchmark (2023) stresses that digital public services must remain inclusive and user-centric, warning against 'digital-only' approaches that risk excluding vulnerable groups, particularly

8 The example of Slovenia illustrates how its network of bank branches has significantly contracted in recent years. This trend reflects the rapid digitalisation of banking services and the reduction in banks' physical presence, leaving an increasing number of users with access to banking services primarily through digital channels. Such developments particularly affect individuals who either lack access to digital technologies or deliberately choose not to use them.

9 An illustrative example is Slovenia, where recent amendments to legislation on administrative procedures preserve the freedom of natural persons to choose between digital and non-digital interaction with public authorities, whereas legal persons are, for instance, subject to a mandatory electronic service.

older persons, rural populations, and persons with disabilities. Likewise, the Organisation for Economic Co-operation and Development (2020, pp. 10–11) has emphasised that effective digital government requires 'multi-channel service delivery', which ensures that offline access remains available for essential public services, including social protection, healthcare, and administrative procedures.

Ensuring offline alternatives thus involves more than retaining legacy procedures; it requires deliberate policy choices aimed at institutional resilience and democratic pluralism. Measures may include co-locating multiple public services in shared physical spaces, enabling assisted access for administrative procedures, and maintaining analogue options for payments, applications, and information requests. Such arrangements not only support non-users but also strengthen systemic robustness during crises, when digital infrastructures may prove insufficient or inaccessible.

Ultimately, the availability of offline pathways constitutes a core condition for preventing the marginalisation of non-users, as discussed further below. Without them, digital citizenship risks evolving from an enabling framework into a subtle form of coercion, in which participation in social, economic, and political life becomes contingent on digital conformity. Respecting the right not to use the internet therefore requires embedding choice into the design of public institutions themselves, ensuring that digital transformation enhances rather than constrains individual autonomy.

As society becomes increasingly digitalised, individuals who choose not to use the internet may face a new form of social exclusion. Ożóg and Puchta (2025b, pp. 97, 99) argue that this digital marginalisation can manifest in both vertical and horizontal dimensions: in the former, non-users may be excluded from access to public services and public administration, including healthcare, education, and administrative procedures, as these services migrate online. In the horizontal dimension, exclusion occurs as essential aspects of everyday life, such as shopping, banking, accessing news, and engaging with media, become predominantly digital. Unlike traditional forms of social exclusion, this new type arises not from personal incapacity or social discrimination alone, but from the structural shift of societal functions into digital spaces. Preventing such marginalisation requires policies that maintain offline alternatives, provide adequate support to marginalised groups, and respect the right not to use the internet, thereby ensuring that digital citizenship protects both the positive and negative dimensions of fundamental rights.

Conclusion

The rapid digital transformation of contemporary societies has profoundly reshaped the conditions under which citizenship is exercised. Within the European Union in particular, digitalisation is no longer perceived merely as a technological

development but as a structural shift affecting democracy, public administration, economic participation, and the exercise of fundamental rights. Against this background, the concept of digital citizenship has emerged as a framework intended to empower individuals to participate meaningfully in social and political life in an increasingly digital environment. At the same time, however, the very success of digital integration policies has revealed a normative tension: if participation in public life becomes predominantly digital, what space remains for those who, by choice or necessity, remain offline?

This article has argued that the right not to use the internet is not a marginal or antagonistic claim directed against digital progress; rather, it constitutes an essential and logically coherent element of digital citizenship properly understood. Digital citizenship, as embedded in the European legal order, derives its normative force from fundamental rights such as privacy, self-determination, freedom of expression, equality, and the right to good administration. These rights are not unidimensional: they protect both the positive freedom to act and the negative freedom to refrain. Just as freedom of expression includes the right not to speak and freedom of religion includes the right not to believe, so too must the right of access to the internet encompass the freedom not to engage with it.

The European approach to digital transformation, encapsulated in the Digital Decade agenda and the Digital Compass, places a strong emphasis on inclusion, digital skills, infrastructure, and the digitalisation of public services. These objectives are legitimate and necessary. Bridging the digital divide, whether understood as a lack of access, lack of skills, or unequal benefits, remains a central task of contemporary social policy. Without effective access to digital tools, individuals risk exclusion from democratic participation, labour markets, education, and public discourse. In this sense, digital citizenship has an undeniable social rights dimension: it requires the state to take positive steps to ensure meaningful access to digital environments.

However, the analysis conducted in this article demonstrates that inclusion cannot be equated with compulsion. When 'digital by default' policies evolve into 'digital-only' practices, the enabling logic of digital citizenship risks turning into digital coercion. Such coercion may not be explicit, but it operates structurally when essential public or private services are only accessible online. In these circumstances, the right to use the internet is transformed de facto into an obligation, and individuals who remain offline, particularly the elderly, persons with disabilities, rural residents, or economically disadvantaged groups, face the risk of vertical and horizontal marginalisation.

From the perspective of European human rights law, such outcomes are difficult to justify. Article 8 of the ECHR protects personal autonomy and lifestyle choices, which encompass decisions regarding technological engagement. Article 10 safeguards not only access to information but also the pluralism of communication channels. Article 41 of the EU Charter requires that public administration remain

accessible, fair, and responsive, irrespective of the medium. These guarantees collectively indicate that digitalisation must remain subordinate to human dignity and individual choice.

Recognising the right not to use the internet does not imply rejecting digital innovation, nor does it entail freezing public administration in analogue form. Rather, it requires designing systems that are inclusive without being coercive. This includes maintaining functional offline alternatives for essential public services, ensuring multi-channel communication, and embedding proportionality analysis into digital policymaking. The right not to use the internet, like other qualified rights, is not absolute; in exceptional circumstances, such as public health emergencies or compelling public interests, temporary limitations may be justified, provided they satisfy the requirements of legality, necessity, and proportionality. Yet such limitations must remain the exception, not the rule.

Importantly, the recognition of offline autonomy has both practical and symbolic significance. Practically, it offers legal clarity and policy guidance, preventing the gradual erosion of non-digital pathways. Symbolically, it reaffirms that technological progress is a means rather than an end. The digital transformation of Europe is intended to serve people, not to redefine the conditions of belonging in ways that exclude those who diverge from dominant technological norms.

Digital citizenship should be understood as a framework of rights that protects participation, competence, and access while simultaneously safeguarding autonomy and pluralism. Its legitimacy depends on preserving the balance between empowerment and restraint, and between integration and freedom of choice. The future of European digital policy must rest on a human-centred constitutionalism of the digital age. Such an approach recognises that the same fundamental rights apply online and offline, and that the expansion of digital opportunities must not result in new forms of exclusion. By embedding the right not to use the internet within the broader architecture of digital citizenship, the European Union can ensure that digital transformation strengthens democracy rather than narrowing the space of individual freedom.

REFERENCES

Bennett, W. L. (2007) 'Changing Citizenship in the Digital Age' in Bennett, W. L. (ed.) Civic Life Online: Learning How Digital Media Can Engage Youth, Cambridge, MA: MIT Press, 1–24.

Chen, Y. C., & Gant, J. (2001). Transforming local e-government services: The use of application service providers. *Government Information Quarterly*, *18*, 343–355.

Council of Europe. (n.d.). *Digital citizenship education*. https://www.coe.int/en/web/education/digital-citizenship-education

Custers, B. (2019). Nieuwe digitale (grond)rechten. *Nederlands Juristenblad*, *44*, 3288–3295. https://doi.org/10.2139/ssrn.4014541

de Hert, P., & Kloza, D. (2012). Internet (access) as a new fundamental right: Inflating the current rights framework? *European Journal of Law and Technology*, *3*(3). https://ejlt.org/index.php/ejlt/article/view/123

de Moraes, J. A., & de Andrade, E. B. (2015). Who are the citizens of digital citizenship? *International Review of Information Ethics*, *23,* 4–19.

Emejulu, A., & McGregor, C. (2019). Toward a radical digital citizenship in digital education. *Critical Studies in Education*, *60*, 131–147.

European Commission. (2021a). *2030 Digital Compass: The European way for the digital decade*. https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52021DC0118

European Commission. (2021b). *State of the Union: Commission proposes a path to the digital decade to deliver the EU's digital transformation by 2030*. https://ec.europa.eu/commission/presscorner/detail/en/ip_21_4630

European Commission. (2023). *eGovernment benchmark 2023: Entering a new digital government era*. Publications Office of the European Union. https://digital-strategy.ec.europa.eu/en/library/egovernment-benchmark-2023

European Parliament, Council of the European Union, & European Commission. (2023). *European declaration on digital rights and principles for the digital decade (2023/C 23/01)*. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32023C0123(01)

Hintz, A., Dencik, L., & Wahl-Jorgensen, K. (2019). *Digital citizenship in a datafied society*. Polity Press.

Isin, E., & Ruppert, E. (2015). *Being digital citizens*. Rowman & Littlefield.

Isman, A., & Güngören, Ö. C. (2014). Digital citizenship. *Turkish Online Journal of Educational Technology*, *13*(1), 73–77.

Jenkins, H., & Carpentier, N. (2013). Theorising participatory intensities: A conversation about participation and politics. *Convergence*, *19*(3), 265–286.

Jóźwicki, W., & Szoszkiewicz, Ł. (2025). Non-use of the internet as a human rights enabler? The curious cases of the right to privacy and the right to health. In D. Kloza, E. Kużelewska, E. Lievens, & V. Verdoodt (Eds.), *The right not to use the internet: Concept, contexts, consequences* (pp. 106–120). Routledge. https://doi.org/10.4324/9781003528401–7

Judgment of the European Court of Human Rights of 24 September 2019 on the case of *Vučina v. Croatia*, application no. 58955/13.

Karaboga, M., Matzner, T., Obersteller, H., & Ochs, C. (2017). Is there a right to offline alternatives in a digital world? In Leenes, R., van Brakel, R., Gutwirth, S., De Hert, P. (Eds.), *Data protection and privacy: (In)visibilities and infrastructures* (pp. 31–50). Springer.

Kaur, H. (2021). Protecting internet access: A human rights treaty approach. *Brooklyn Journal of International Law*, *46*(2), 767–806.

Kloza, D. (2024). The right not to use the internet. *Computer Law & Security Review*, *52*, 105907. https://doi.org/10.1016/j.clsr.2023.105907

Kloza, D., Kużelewska, E., Lievens, E., & Verdoodt, V. (Eds.). (2025). *The right not to use the internet: Concept, contexts, consequences*. Routledge.

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

Kużelewska, E., Tomaszuk, M., & Malinowski, D. (2025). The elderly digital divide: Digital exclusion versus the right not to use the internet. *International Journal for Semiotics of Law*. https://doi.org/10.1007/s11196–025–10334–4

Lucchi, N. (2013). *The role of internet access in enabling individuals' rights and freedoms* [EUI RSCAS Working paper 47]. European University Institute Robert Schuman Centre for Advanced Studies. https://www.researchgate.net/publication/241276736_The_role_of_Internet_access_in_enabling_individual's_rights_and_freedoms

Mossberger, K., Tolbert, C. J., & McNeal, R. S. (2007). *Digital citizenship: The internet, society and participation*. MIT Press.

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.

Nowina-Konopka, M. (2017). The European concept of e-governance in the light of European Commission indicators. *Zeszyty Prasoznawcze*, *60*(2), 329–349.

OECD. (2020). *The OECD digital government policy framework: Six dimensions of a digital government*. https://www.oecd.org/content/dam/oecd/en/publications/reports/2020/10/the-oecd-digital-government-policy-framework_11dd6aa8/f64fed2a-en.pdf

Ożóg, M., & Puchta, R. (2025a). The right not to use the internet and protection against the digital divide: Some preliminary remarks. *Białostockie Studia Prawnicze*, *30*(4), 9–23. https://doi.org/10.15290/bsp.2025.30.04.01

Ożóg, M., & Puchta, R. (2025b). The right not to use the internet: Toward a negative digital freedom in Polish law. In D. Kloza, E. Kużelewska, E. Lievens, & V. Verdoodt (Eds.), *The right not to use the internet* (pp. 92–105). Routledge. https://doi.org/10.4324/9781003528401–6

Pangrazio, L., & Sefton-Green, J. (2021). Digital rights, digital citizenship and digital literacy: What's the difference? *Journal of New Approaches in Educational Research*, *10*(1), 15–27. https://doi.org/10.7821/naer.2021.1.616

Passaglia, P. (2022). Behind the curtain: Questioning the right to access the internet. *Völkerrechtsblog*. https://doi.org/10.17176/20221017–110251–0

Passaglia, P. (2025). Conceptualising the right to access the internet and its impact on the right not to use it. In D. Kloza, E. Kużelewska, E. Lievens, & V. Verdoodt (Eds.), *The right not to use the internet* (pp. 29–43). Routledge. https://doi.org/10.4324/9781003528401–4

Pollicino, O. (2020). The right to internet access. In A. Von Arnauld, K. Von der Decken, & M. Susi (Eds.), *The Cambridge handbook of new human rights* (pp. 263–275). Cambridge University Press. https://doi.org/10.1017/9781108676106.021

Ribble, M., & Bailey, G. (2007). *Digital citizenship in schools*. ISTE.

Right to Offline Coalition. (2024). *Essential services must be accessible, even offline*. https://righttooffline.eu

Robles, M. (2009). *Digital citizenship*. Editorial UOC.

Rossi, J. (2025). Is there a right to be offline 'for no reason' in France? In D. Kloza, E. Kużelewska, E. Lievens, & V. Verdoodt (Eds.), *The right not to use the internet* (pp. 76–91). Routledge. https://doi.org/10.4324/9781003528401–6

Rutkowska-Tomaszewska, E., & Gałązka, P. (2024). The role of European supervisory authorities in consumer protection standard setting. *Studies in European Affairs*, *28*(2), 223–232.

Shelley, M., Thrane, L., Shulman, S., Lang, E., Beisser, S., Larson, T., & Mutiti, J. (2004). Digital citizenship: Parameters of the digital divide. *Social Science Computer Review*, *22*(2), 256–269.

Susi, M. (2025). Framing the right not to use the internet. In D. Kloza, E. Kużelewska, E. Lievens, & V. Verdoodt (Eds.), *The right not to use the internet* (pp. 44–70). Routledge. https://doi.org/10.4324/9781003528401–6

SwissInfo. (2025a). *'It's political': Why some people refuse to have a smartphone*. https://www.swissinfo.ch/eng/digital-democracy/its-political-why-some-people-refuse-to-have-a-smartphone/89012366

SwissInfo.(2025b).*HowSwissfederalismishelpingtheriseofanewdigitalright*.https://www.swissinfo.ch/eng/digital-democracy/how-swiss-federalism-is-helping-the-rise-of-a-new-digital-right/89023201

Terzis, G. (2025). Ethical meditations for a human right to an analogue life. In D. Kloza, E. Kużelewska, E. Lievens, & V. Verdoodt (Eds.), *The right not to use the internet* (pp. 29–43). Routledge. https://doi.org/10.4324/9781003528401–6

Thrane, L., Shelley, M., Shulman, S., Beisser, S., & Larson, T. (2004). E-political empowerment: Age effects or attitudinal barriers. *Journal of E-Government*, *1*(4), 21–37.

Tomalty, J. (2017). Is there a human right to internet access? *Philosophy Now*, *118*, 8–11. https://philosophynow.org/issues/118/Is_There_A_Human_Right_To_Internet_Access

United Nations Human Rights Council. (2016). *The promotion, protection and enjoyment of human rights on the internet (A/HRC/32/L.20)*. https://documents-dds-ny.un.org/doc/UNDOC/LTD/G16/108/02/PDF/G1610802.pdf

Warren, S., & Brandeis, L. (1890). The right to privacy. *Harvard Law Review, 4*(5), 193–220.

Vromen, A. (2017). *Digital citizenship and political engagement*. Palgrave Macmillan.

Yao, C., & Quinn, P. (2025). Bridging the digital divide. In S. Serpa & A. I. Santos (Eds.), *Digital equity and literacy* (pp. 1–24). IntechOpen. https://doi.org/10.5772/intechopen.1011614

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

sciendo

DOI: 10.15290/bsp.2026.31.01.05

Received: 30.06.2025
Accepted: 08.01.2026

Ermanno Petrocchi
University of Macerata, Italy
e.petrocchi1@unimc.it
ORCID ID: 0009–0001–8298–3076

Letizia Conte
University of Macerata, Italy
l.conte1@unimc.it
ORCID ID: 0009–0006–8932–5515

Civic Engagement in the AI Age: The Role of Digital Activism in Fostering Democratic Technologies

Abstract: This paper examines the crucial role of activism and civil society in strengthening democratic values, particularly in the context of the contemporary challenges posed by artificial intelligence (AI). People's involvement through different forms of associative participation fosters accountability and social capital, essential for democratic resilience. However, the rise of AI poses risks, including manipulation through disinformation, deepfakes, and privacy violations, which threaten democratic processes and fundamental rights. In response to such threats, digital activism emerges as an essential tool, not only for mobilising people but also for steering technological development towards more inclusive and responsible forms. The article argues that digital activism should not be limited to awareness-raising or AI literacy initiatives, but rather should be recognised as a proactive force in the definition of an ethical AI consistent with democratic values. In this framework, participatory design represents a fundamental methodological tool; indeed, it aims at involving different stakeholders in AI design processes to create more responsible technologies. Therefore, through the active involvement of digital activism associations in AI decision-making processes, people can contribute to the democratic control of technologies and the safeguarding of fundamental freedoms. Just as civic engagement has historically strengthened democratic institutions, digital activism therefore has the potential to guide AI development towards fairer and more transparent and accountable technological futures.

Keywords: civil society, digital activism, democracy, AI ethics

Introduction

Civic activism and participation are among the key driving forces in the strengthening of democratic systems. Civil society, through non-governmental organisations, social movements, and other forms of associative participation, is a major player in ensuring the accountability of institutions and their capacity to respond effectively to people's needs. In particular, civic participation plays an important role in the formation of social capital, strengthening cohesion among community members and promoting skills essential for political engagement, such as information skills, tolerance, and a sense of belonging (Putnam, 1995).

In the current era, marked by technological acceleration and in particular the spread of artificial intelligence (AI), new and complex challenges for democracy have emerged. AI-based technologies can indeed be used to manipulate public opinion through disinformation, to compromise the integrity of electoral processes, and to jeopardise fundamental rights such as privacy and individual autonomy (Coeckelbergh, 2024). This paper argues that despite the challenges posed by the widespread use of AI technologies, it is precisely in this context that digital activism can emerge as a pivotal tool not only for the defence of democratic freedoms but also for the construction of a more just and inclusive technological ecosystem.

Among the various approaches to the responsible development of digital technologies, participatory design represents a particularly relevant perspective. This approach is based on the active involvement of stakeholders, such as experts, technologists, end users, and members of society in a broader sense, in the design and development processes of technologies.[1] The aim of participatory design is to overcome technocratic and top-down models, instead promoting collaborative practices that strive to co-create more inclusive, contextualised, and socially just solutions (Delgado et al., 2023). Participatory design is not limited to collecting post-hoc feedback, but rather requires continuous and direct involvement, paying particular attention to power inequalities and the technology's ethical and social impacts. Participatory design therefore emerges as a promising strategy to mitigate the risks of automated systems, improve transparency, and ensure the accountability of the actors involved (Delgado et al., 2023; Zytko et al., 2022).

In this context, this paper argues that digital activism, framed within the logic of participatory design, can constitute a privileged channel for people's involvement in AI systems' development processes. In this sense, activism represents not only a form of political mobilisation but a concrete way through which individuals can take an

1 We have decided to use alternative terms to 'citizens' in order to avoid excluding individuals who do not hold formal citizenship status.

active role in the co-creation of AI technologies. Similarly to how associative participation has historically strengthened traditional democracy, the involvement of civil society in the development of AI can help orient this technology towards democratic values (Brynjolfsson et al., 2025). The direct involvement of activists and experts in decision-making processes can enable them to shape AI technologies that are more inclusive and sensitive to their social impacts.

For these reasons, this paper proposes interpreting digital activism not simply as a form of mobilisation, protest, or denunciation, but as an active source of technological design, capable of contributing to the realisation of reliable, accountable, and democratically aligned AI systems. Our goal is to show how civic engagement through digital activism can be a concrete way to democratise AI and protect fundamental rights in a rapidly evolving technological context.

To this end, the paper is structured as follows: Section 1 analyses the role of civic participation in democratic societies, highlighting how activism has also evolved in response to technological changes and introducing the concept of digital activism. Section 2 discusses the main risks posed by AI to democratic systems. Section 3 delves into the participatory design approach, emphasising how digital activism can be integrated within this approach to empower citizens in shaping technological development. It also underscores the responsibility of democratic institutions in fostering such activism as a means of supporting participatory technology design. Section 4 offers some concluding remarks.

1. The role of active participation in shaping democratic societies

The transformative role of civil society associations and social movements has long attracted scholarly interest due to their ongoing adaptation to political and social change. Particular attention has been paid to the contribution that the participation of activists offers to the creation of conditions for authentic democracy, by fostering social solidarity, reinforcing civic bonds, and enhancing the effectiveness of public policy through multiple activities (Maloney & Van Deth, 2010).

Tocqueville already highlighted the importance of associationism for the life of American democracy, highlighting some of its characteristics and effects that are still considered valid (Edwards et al., 2001). He reflected in particular on how the American associations he studied guaranteed a fundamental pre-political socialisation, spreading the spirit of cooperation, solidarity, and civic engagement among the participants (Biorcio & Vitale, 2016). Many scholars have re-proposed his idea of associations as 'schools of democracy', valuing especially the role of political socialisation that associative participation can play.

However, in contemporary democracies, the relationship between associations and politics is much more complex and has changed significantly in recent decades.

The socialisation of members is no longer the sole function that associations serve within a participatory democracy; today, they function as collective actors in the public sphere to directly influence policies with various forms of initiatives and mobilisations, to put pressure on governments, but also to direct the production of public goods (Biorcio & Vitale, 2016).

In this sense, Putnam (1995), introducing the concept of 'social capital', highlighted the importance of associative participation as an essential condition for the proper functioning of democracy. This term refers to a set of elements such as relationships based on trust, the rules that govern collective life, and networks of civic associations. These factors contribute to making social organisation more efficient, favouring shared initiatives and decisions made collaboratively. The existence of a high level of social capital in a community should therefore trigger a virtuous circle, thanks to which it can grow further, guaranteeing the best conditions for democratic life.

Associative participation also increases the resources available for political participation: civic competence, information, membership in social networks, a sense of personal effectiveness, and the ability to act politically (Binder, 2020). Active participation fosters the acquisition of democratic decision-making methods, directing individuals towards dealing with issues of collective interest and promoting the construction of bonds based on trust and reciprocity. Engaging in socially relevant activities, with tangible and recognisable outcomes, helps to strengthen the self-efficacy and self-esteem of the participants. This process reflects a reworking of the value systems of activists, who tend to develop a greater awareness of and attention towards the political sphere, public policies, and institutional decisions (Maloney & Van Deth, 2010).

Since the 1980s, the rise of neoliberalism and globalisation has contributed to an erosion of faith in state intervention, leading to a reconfiguration of civil society's role. Indeed, civil society organisations have increasingly assumed functions traditionally carried out by political parties and institutions, such as mediating social demands and fostering political socialisation, especially among young people (Biorcio & Vitale, 2016).

In addition, the technological revolution – from the emergence of social media to the development of AI – has deeply transformed the landscape of activism, reshaping its tools, strategic approaches, and associated risks. This constantly evolving context even makes it difficult to precisely delineate the conceptual boundaries of emerging digital activism, as the rapid transformations taking place make its definition continuously provisional and subject to redefinition (Özkula, 2021a).

In this scenario, activist associations do not limit themselves to using digital technologies as operational tools, but rather take on a crucial role in monitoring, reporting, raising awareness of, and disseminating information about the social and political effects of technological innovations. These organisations, however, are themselves exposed to critical issues deriving from the use of these tools, including 'invisibilisa-

tion' phenomena, i.e. the reduced visibility of politically sensitive or dissenting content within digital platforms, and surveillance practices, namely the systematic monitoring, data collection, and profiling of activists by the state or private companies (Dencik et al., 2016; Etter & Albu, 2021; Lane et al., 2017; Özkula, 2021a). In the following section, the distinctive features of contemporary digital activism and the specific functions performed by modern social capital in this new digital ecosystem will be explored.

1.1. Activism in the digital age: Opportunities and limits

The rise of social media and digital technologies over the past decades has significantly reshaped the landscape of civic engagement and activism (Bennett & Segerberg, 2012). Civil society actors are increasingly using digital functionalities to articulate political claims, reach broader audiences, and challenge dominant narratives. Indeed, these tools have expanded the communicative and organisational capacities of social movements, enabling wider participation and more agile mobilisation strategies, as well as the diversification of voices within the public sphere (Castillo Esparcia et al., 2023). However, this transformation has also prompted critical reflections on the efficacy and nature of this new form of digital activism in a lot of scholarly literature in recent decades (Helmond, 2015; Mora, 2014; Özkula, 2021a, 2021b, 2021c).

In general terms, digital activism can be defined as a form of political activism that develops through the internet (McCaughey & Ayers, 2003). Its defining actions mirror traditional practices of activism (such as petitions and protests) while also employing digital technologies to support or organise offline activities, such as the promotion of events through social media. Over the past two decades, this type of activism has fostered high levels of interaction and interconnection, for instance through tweets, posts, chats, and sharing of content, especially user-generated content, across geographical and institutional boundaries (Özkula, 2021b).

However, the terminology associated with this phenomenon is ambiguous, reflecting the constant evolution of digital technologies. Indeed, there are many alternative expressions according to the tools used: among these are 'online activism', 'social media activism', 'internet activism', and 'hashtag activism' (Mora, 2014). In this context, the term 'digital activism' is configured as an umbrella term, as it encompasses these different forms and aligns with recent linguistic trends that favour the use of the term 'digital' over 'online', in recognition of the increasingly pervasive processes of advanced digitisation (Özkula, 2021b, 2021c).

Özkula (2021b) distinguishes practices of digital activism in five main categories: (i) advocacy and political commentary, (ii) recruitment and movement building, (iii) organisation and coordination, (iv) online direct action, hacktivism, and civil disobedience, and (v) research and documentation. The latter category in particular can be fundamental strategic tools for activist action, as they are functional to the dissemination of information relating, for example, to human rights violations. These activities can be carried out directly, e.g. through the use of mobile phones, or conveyed through

traditional media (McCaughey & Ayers, 2003). This also includes practices such as the disclosure of confidential information, election observation, countering disinformation and electoral fraud, as well as forms of 'sousveillance', i.e. bottom-up surveillance practices, in which citizens document and publicise abusive behaviour by state institutions, such as police forces or government authorities. Although it is a matter of debate whether such documentation activities can be considered forms of activism in their own right, they are often carried out in support of activist action or with the explicit intention of expressing dissent, as in the emblematic case of Wikileaks (Özkula, 2021b).

As we will see in Section 4, this is one of the most recurrent strategies in the cases of civil society organisations that constantly carry out studies, monitoring, denunciation, and awareness work regarding the political and social risks of the use of AI tools.

Although digital activism offers numerous opportunities for mobilisation and participation, it is not immune to the risk of incurring the same anti-democratic logic of control and limitation against which it often stands in opposition. In particular, the activism conveyed through social media platforms is strongly influenced by the dynamics of visibility imposed by the techno-commercial infrastructures that regulate their operation. As highlighted by Helmond (2015), the increasing platformisation of digital public spheres has concentrated decision-making power over content circulation in the hands of private actors, whose moderation mechanisms are frequently opaque and lack effective accountability.

As a result, activists are forced to operate within digital spaces increasingly determined by non-transparent algorithmic logics, exposing themselves to the risk of the invisibility of their messages and communicative precariousness due to the automatic classification of content (Etter & Albu, 2021). The surveillance of activists by platforms represents, in this context, a crucial dimension to be analysed, given the centrality assumed by these tools in the configuration of contemporary protests. Facebook, for instance, is configured as a primary hub for the communication, mobilisation, and organisation of activist networks. Nevertheless, activist engagement on Facebook generates digital traces, and the platform's expansive operational reach intensifies the vulnerabilities linked to digital protest, amplifying the harmful consequences of online surveillance. This form of surveillance can inhibit free expression and lead to the unequal restriction of civil rights (Nurik, 2022). This case highlights how the evolution of technologies, especially those that are AI-based, has significant implications that require careful critical analysis.

2. How AI undermines democracy

The massive adoption of AI, and more recently generative AI, in the public and political space entails several risks that go far beyond purely technical concerns. These systems are not mere technical tools but devices that mediate access to knowl-

edge and help structure the conditions of democratic debate. As Coeckelbergh (2024) and Mentxaka et al. (2025) have pointed out, the political risks of large-scale adoption of AI systems are multiple and profound.

One of the most immediate dangers lies in the ability of generative AI systems to produce fake content. Such content can take the form of deepfakes, i.e. artificial videos capable of simulating faces, voices, and movements in an extremely realistic manner, or hallucinations, i.e. errors typical of large language models (LLMs) that generate seemingly plausible statements that lack any real substance (Huang et al., 2025; Westerlund, 2019). These phenomena, which may be accidental or deliberately orchestrated, fuel the production of fake news, targeted attacks, and political disinformation campaigns (Schick, 2020). The speed and scale with which such content is generated and disseminated pose a direct threat to the integrity of public discourse and citizens' capacity to form opinions based on verifiable facts (Coeckelbergh, 2025a).

For democracy to function effectively, it presupposes that citizens can exercise a minimum of cognitive autonomy, the ability to critically evaluate information and make independent judgements. However, increasing exposure to misleading content and uncritical interaction with AI systems undermines this capacity. As pointed out by Rini (2020), Fallis (2021), and Coeckelbergh (2025b), one of the main risks of the use of generative AI systems is that of the progressive weakening of individual epistemic agency, with direct consequences on the quality of civic participation and democratic deliberation.

In parallel, the use of AI in social media and search engines encourages the formation of epistemic bubbles and echo chambers, closed digital environments in which users are exposed almost exclusively to content that confirms their pre-existing beliefs (Nguyen, 2020). This hinders encounters with divergent opinions and inhibits critical confrontation, fuelling a polarised worldview (Croce & Piazza, 2022). Under such conditions, dissent turns into hostility, dialogue gives way to monologue, and democratic cohesion disintegrates.

A further risk, less obvious but equally dangerous, is the self-referential repetition of knowledge. When LLMs are trained on content generated by other models, a closed circuit is created in which information reproduces itself without innovating. This phenomenon, referred to as 'epistemic incest', undermines society's ability to receive new signals, elaborate answers to emerging problems, or include tacit or uncodified forms of knowledge (Coeckelbergh, 2025a).

In brief, the uncontrolled and opaque use of AI systems not only jeopardises the quality of information but also profoundly affects the very structure of democratic deliberation. In the absence of regulation, critical education, and transparent digital infrastructures, AI risks becoming an instrument of cognitive fragmentation and the erosion of civic bonding, rather than being an ally of democratic progress.

3. Reframing participation: Digital activism, democratic values, and the role of participatory design in the AI era

The democratisation of AI cannot be delegated solely to experts but requires inclusive participatory processes capable of redistributing technological power and fostering systems that are fairer, more transparent, and responsive to collective needs. Individuals should be empowered with the capacity to engage in informed deliberation and exert influence over AI development and use in ways that are more responsive to collective needs.

In contemporary digitised society, participation has emerged as a widespread promise – manifested in practices ranging from crowdfunding to user-generated content on social media – often seen as a driver of democratic innovation. Yet this promise coexists with a contradictory trend: the increasing centralisation of capital, infrastructure, and data through large-scale platforms, which undermines core democratic ideals such as civic participation, data ownership, and privacy (Smith et al., 2017).

In a context where digital infrastructures, in particular those underpinned by AI, are increasingly governed by opaque logics, it becomes essential to provide users with critical literacy and awareness of the associated risks. Several civil society organisations have begun to play a crucial role in this regard, offering tools for public education, conducting oversight, and fostering democratic scrutiny. These initiatives reflect a broader effort to embed values such as equity, accountability, and transparency in the development and deployment of digital technologies (Milan, 2015).

Multiple perspectives on participation show its evolving relevance across contemporary contexts, highlighting how the democratic ideals underlying participatory design continue to serve as effective tools for critical engagement.

Participatory design, with its emphasis on values, aspirations, and the sociopolitical contexts in which technologies are developed, provides depth and direction often overlooked in the dominant discourse, which is focused primarily on innovation or efficiency (Smith et al., 2017).

This paper contends that activist networks – already engaged in monitoring, raising awareness, and pressuring for ethical technological practices – should be included as key actors within participatory processes (Tsai & Pentland, 2025). These networks provide valuable perspectives both in influencing public policy and in guiding users towards more informed and responsible use of AI-based tools. Examples like Algorithm Watch, which will be analysed in the following section, demonstrate how activist organisations are strategically mobilising various tools to challenge the unchecked expansion of biased algorithms and to contest algorithmic injustices.

A key strategy for achieving this is participatory design, which promotes the inclusion of different actors in AI design and implementation (Delgado et al., 2023; Zytko et al., 2022). Originating from Scandinavian labour movements in the 1970s, it has

evolved into a critical methodology for ensuring that technological systems reflect the values, needs, and experiences of different user communities (Bødker et al., 2004).[2]

In the context of AI, the involvement of activist organisations, particularly those addressing the concerns of historically marginalised or underrepresented communities, in co-design processes can mitigate algorithmic harms and promote socially just outcomes, particularly by tackling epistemic injustices embedded in data practices (D'Ignazio & Klein, 2020; Overton, 2025). As such, participatory design constitutes not only a technique but also an epistemic and political intervention, grounded in subaltern knowledge, local worldviews, and situated experiences, as emphasised also by decolonial and feminist theories of AI ethics (Mohamed et al., 2020; Suchman, 2002). Through these efforts, participatory design contributes to building more pluralistic, just, and democratically aligned technological futures.

Drawing on these opportunities, this article proposes that digital activism should not be limited to raising awareness about the risks of AI or enhancing public literacy; rather, it should be recognised as a central mechanism for fostering inclusive and justice-oriented AI development (Castillo Esparcia et al., 2023; Özkula, 2021c). By integrating activist participation into AI decision-making processes, democratic engagement can be enhanced and technological systems can be aligned more closely with fundamental rights and collective values. In this light, digital activism, when reformulated through the lens of participatory design, emerges as a transformative force in the democratic governance of algorithmic systems.

Nonetheless, incorporating justice-oriented participation into AI development presents significant challenges, predominantly within capitalist frameworks that prioritise scalability and efficiency (Sloane et al., 2020). As machine-learning systems expand, they often lose the contextual sensitivity achieved through previous participatory efforts (Boyd & Crawford, 2012; Selbst et al., 2019). Despite these constraints, participatory design, anchored in principles of justice, transparency, and accountability, remains a vital tool aligned with the aims of digital activism, offering a pathway towards more equitable and democratic technological ecosystems.

Indeed, this type of activism represents a privileged channel through which members of society can be included in technology co-design processes. After all, without a supportive association or network, it is extremely difficult for the individual to find a way to speak out about technology, bring forward their demands, and thus be considered from the early stages of AI development processes. Digital activism in this sense takes the form of an accessible and collective way of participating, which allows even those who do not work in the tech sector to shape the technological tools they use in their everyday life.

2 The reference to the Scandinavian labour model lends substantial support to our argument that democratic activists and affiliated organisations can mitigate the societal risks and abuses associated with AI.

4. Institutions' responsibilities

In the design of AI technologies that increasingly permeate everyday life, public institutions can no longer confine themselves to ex-post regulation or the passive adoption of technical tools. Instead, they must assume an active role in promoting participatory practices that engage members of society in the definition, oversight, and evaluation of digital infrastructures (Coeugnet et al., 2023).

As previously discussed, digital activism emerges as a crucial actor in this regard. Recognising the civic value of digital activism, however, is not sufficient in itself (Stamboliev, 2023); what is needed is a deliberate institutional effort to create the conditions under which this form of participation can flourish and exert real influence on design and governance processes. In this regard, two fundamental responsibilities for institutions follow from these considerations: the first is to build an institutional ecosystem in which digital activism associations are recognised as legitimate interlocutors and included in the design, implementation, and monitoring processes of AI systems. The second, more general, is to actively encourage the spread of digital activism. Digital activism in fact constitutes not only a channel for citizens to participate in the co-creation of technologies but also assumes a more educative role, i.e. that of a driver for the development of the skills needed to critically understand and manage digital technologies. Indeed, in light of the risks to the democratic system highlighted in the previous sections, there is a clear need to promote greater public awareness of how AI works, the skills required to consciously interact with such systems, and the tools available to defend against asymmetries of digital power. This is the only way to strengthen democratic resilience and ensure informed, inclusive, and active participation in today's algorithmic society.

Institutions can therefore adopt some concrete strategies to support this dual role of digital activism and promote a more participatory and democratic technological design:

Involve civic actors in decision-making processes on AI, algorithms, and data use (Borchers, 2024). This means including associations of digital activism in committees, public forums, and regulatory bodies where guidelines, standards, and regulations related to the use of AI technologies are defined. This type of involvement favours pluralist deliberation, in which technical knowledge is confronted with the ethical, social, and territorial needs expressed by the community.

Open co-design bodies to digital activists (Feltrero & Osuna-Acedo, 2023). Public technologies, such as digital platforms, surveillance systems, and predictive intelligence tools, should be designed through structured participatory processes that include the different voices of the community. These bodies can function as hybrid spaces where user experiences are shared, concrete needs are defined, ethical implications are assessed, and sustainable, accessible, and inclusive solutions are co-designed.

Fund educational projects and awareness-raising campaigns (Hsu et al., 2022; Stamboliev, 2023). Critical digital literacy is a prerequisite for effective participation; institutions can support digital activism associations to promote educational programmes, public workshops, information toolkits, and social campaigns to help people understand how algorithms work, what data is used, and what the risks and opportunities of AI are, not just providing technical skills but educating aware individuals capable of influencing the public debate.

Favour bottom-up initiatives to carry out algorithmic audits and ethical and social impact assessments of public technologies. Administrations can enter into partnerships with independent organisations and digital activists to conduct transparent audits of the functioning of algorithmic systems in use by public bodies or outsourced services. Such collaborations can make it possible to identify bias, discriminatory effects, privacy risks, and indirect impacts on social cohesion. Participatory auditing can turn into a tool of collective accountability, capable of giving citizens back an active role in the surveillance of technological power.

These actions, if implemented consistently and continuously, can help transform digital activism from a marginal phenomenon to a structural component of technological democracy, ensuring in this way that decisions on the digital future of societies are addressed in an open, accountable, and inclusive manner (Spielkamp, 2017).

Examples already exist of the educative function of digital activism. One is Algorithm Watch, an independent non-profit organisation engaged in the monitoring, analysis, and public communication of automated decision-making systems. Algorithm Watch exposes the opacity and discriminatory risks inherent in algorithms used in the public and private spheres, promotes the adoption of ethical, transparent, and fair practices by institutions, and offers information, training, and support tools for citizens and decision-makers (Stark et al., 2020). By collaborating with academic bodies, media, and policymakers, this organisation demonstrates how digital activism can act as a mediator between technology, society, and politics, facilitating a more open and knowledgeable dialogue on issues of automation and algorithmic governance (Cornils, 2020). Algorithm Watch thus embodies the role of activism as an essential civic infrastructure, capable of providing critical expertise and building civic surveillance networks (Loi, 2020).

However, this paper argues that the function of digital activism, well represented by experiences such as that of Algorithm Watch, should not be exhausted in the role of critical observer or facilitator of public awareness. On the contrary, this function can and must be extended to processes of technological co-creation, actively involving civic associations and activist networks in the design phase of the technologies themselves. This marks a paradigm shift, from viewing activism as a downstream watchdog to recognising it as an upstream co-designer. Involving activist organisations from the earliest stages of the technology life cycle means redistributing decision-making power and ensuring that automated systems are not designed solely by

technical experts or industry stakeholders but also by those who represent the public interest, digital rights, and social justice.

From this perspective, digital activism emerges as an indispensable actor in the construction of a truly democratic technological ecosystem, capable not only of denouncing distortions but also of proposing design alternatives oriented towards the common good.

Conclusions

This article has explored how digital activism and participatory design can serve as crucial frameworks to guide the development of AI technologies towards democratic values, social justice, and civic empowerment. Indeed, AI architectures, datasets, and results are deeply rooted in the existing power structures and social biases that arise from historical systems of oppression (Noble, 2018). As these systems become increasingly integrated into governance, the risks they pose to democratic accountability and transparency are amplified significantly. In this context, the defence of democratic principles requires not only institutional reform but also encompasses the technological infrastructures that shape decision-making itself.

Digital activism has emerged as a vital force in this challenge, committing to exposing algorithmic injustice and calling for participatory governance structures that prioritise the voices of marginalised communities (Benjamin, 2019). In this regard, participatory design offers a path to institutionalise democratic engagement in AI design and implementation (Costanza-Chock, 2020).

The paper has argued that if institutions engaged with activist organisations involved in monitoring and raising awareness about the risks of AI, such as Algorithm Watch, from the earliest stages of the technology life cycle, there would be a stronger assurance that automated systems reflect the public interest. This is due to the enhanced capacity of digital activists to connect directly with individuals and represent diverse societal concerns.

By advancing values such as epistemic justice through the recognition of different forms of knowledge and the redistribution of power, these approaches challenge the technocratic rationalities that often dominate AI discourse and practice (D'Ignazio & Klein, 2020).

However, some limitations exist: firstly, participatory practices, while promising, require significant resources, time, and institutional commitment. These conditions are often at odds with the speed and priorities of the tech industry (Boyd & Crawford, 2012). In addition, authentic participation also requires a revisiting of skills and authority, challenging entrenched hierarchies within both the technology and governance sectors.

Despite these limitations, the approaches described stimulate an important reflection on what posture to take with respect to the challenges that AI poses to democratic values. Claiming AI as a democratic space is not just about mitigating damage; it is a matter of expanding the realm of possibilities, of imagining and building technological futures that are just, pluralistic, and respectful of human dignity. Digital activism thus offers a critique of the current trajectory of AI and stands as a model for its democratic transformation, which not only takes into account multiple voices but also works to ensure that individuals can participate equally, with equal respect, in the fight against injustice.

REFERENCES

Benjamin, R. (2019). *Race after technology: Abolitionist tools for the New Jim Code*. Polity.

Bennett, W. L., & Segerberg, A. (2012). The logic of connective action. *Information Communication & Society*, *15*(5), 739–768.

Binder, M. (2020). Enhancing democracy: Can civic engagement foster political participation? *Social Science Quarterly*, *102*(1), 47–68.

Biorcio, R., & Vitale, T. (2016). *Italia Civile: Associazionismo, partecipazione e politica*. Donzelli Editore.

Bødker, K., Kensing, F., & Simonsen, J. (2004). *Participatory IT design*. The MIT Press.

Borchers, M., Gierlich-Joas, M., Tavanapour, N., & Bittner, E. (2024, May). Let citizens speak up: Designing intelligent online participation for urban planning. In Mandviwalla, M., Söllner, M., & Tuunanen, T., (Eds.), *International conference on design science research in information systems and technology* (pp. 18–32). Springer Nature Switzerland.

Boyd, D., & Crawford, K. (2012). Critical questions for big data. *Information Communication & Society*, *15*(5), 662–679.

Brynjolfsson, E., Pentland, A., Persily, N., Condoleezza, R., & Aristidou, A. (2025). Introduction: Artificial intelligence and democracy in America, *The Digitalist Papers: Artificial Intelligence and Democracy in America*, https://www.digitalistpapers.com/essays/introduction.

Castillo Esparcia, A., Smolak-Lozano, E., & Llorent Vázquez, V. (2023). Artificial intelligence and citizen communication: Risk awareness, digital literacy, and civic participation. *Communication & Society*, *36*(1), 1–17.

Coeckelbergh, M. (2024). *Why AI undermines democracy and what to do about it*. John Wiley & Sons.

Coeckelbergh, M. (2025a). LLMs, truth, and democracy: An overview of risks. *Science and Engineering Ethics*, *31*(1), 1–13.

Coeckelbergh, M. (2025b). AI and epistemic agency: How AI influences belief revision and its normative implications. *Social Epistemology*, 40(1), 1–13.

Coeugnet, P., Labatut, J., Duval, J., & Vourc'h, G. (2023). Including citizens through co-design in a participatory research project to explore innovative agro-food systems: The case of future dairy livestock systems. *Frontiers in Sustainable Food Systems*, *7*, 1098295.

Cornils, M. (2020). Designing platform governance: A normative perspective on needs, strategies, and tools to regulate intermediaries. *Algorithm Watch*, *26, 1–88*.

Costanza-Chock, S. (2020). *Design justice: Community-led practices to build the worlds we need*. MIT Press eBooks.

Croce, M., & Piazza, T. (2022). *Che cosa sono le fake news*. Carocci Editore.

Delgado, F., Yang, S., Madaio, M., & Yang, Q. (2023). The Participatory Turn in AI Design: Theoretical Foundations and the Current State of Practice. In Association for Computing Machinery (Ed.), *Proceedings of the 3rd ACM Conference on Equity and Access in Algorithms, Mechanisms, and Optimization*, 37, 1–23. Association for Computing Machinery. https://doi.org/10.1145/3617694.3623261.

D'Ignazio, C., & Klein, L. F. (2020). *Data feminism*. MIT Press eBooks.

Dencik, L., Hintz, A., & Cable, J. (2016). Towards data justice? The ambiguity of antisurveillance resistance in political activism. *Big Data & Society*, *3*(2), 1–12.

Edwards, B., Foley, M., & Diani, M. (2001). Civil society and political context. In B. Edwards, M. Foley, & M. Diani (Eds.), *Beyond Tocqueville: Civil society and the social capital debate in comparative perspective* (pp. 17–31). University Press of New England.

Etter, M., & Albu, O. B. (2021). Activists in the dark: Social media algorithms and collective action in two social movement organizations. *Organization*, *28*(1), 68–91.

Fallis, D. (2021). The epistemic threat of deepfakes. *Philosophy & Technology*, *34*(4), 623–643.

Feltrero, R., & Osuna-Acedo, S. (2023). Social innovation on educational AI developments: A case study on social participation on designing AI generative models for diversity. In Kubincová, Z., Hao, T., Capuano, N., Temperini, M., Ge, S., Mu, Y., Fantozzi, P., & Yang, J. (Eds.), *International symposium on emerging technologies for education* (pp. 16–26). Singapore: Springer Nature Singapore.

Helmond, A. (2015). The platformization of the web: Making web data platform ready. *Social Media + Society*, *1*(2), 1–11.

Hsu, Y. C., Verma, H., Mauri, A., Nourbakhsh, I., & Bozzon, A. (2022). Empowering local communities using artificial intelligence. *Patterns*, *3*(3), 1–7.

Huang, L., Yu, W., Ma, W., Zhong, W., Feng, Z., Wang, H., Chen, Q., Peng, W., Feng, X., Qin, B., & Liu, T. (2025). A survey on hallucination in large language models: Principles, taxonomy, challenges, and open questions. *ACM Transactions on Information Systems*, *43*(2), 1–55.

Lane, D. S., Kim, D. H., Lee, S. S., Weeks, B. E., & Kwak, N. (2017). From online disagreement to offline action: How diverse motivations for using social media can increase political information sharing and catalyze offline political participation. *Social Media + Society*, *3*(3), 1–14.

Loi, M. (2020). People analytics must benefit the people: An ethical analysis of data-driven algorithmic systems in human resources management. *AlgorithmWatch, 1–56*.

Maloney, W. A., & Van Deth, J. W. (2010). *Civil society and activism in Europe*, Routledge.

McCaughey, M., & Ayers, M. D. (2003). *Cyberactivism*. Routledge eBooks.

Mentxaka, O., Díaz-Rodríguez, N., Coeckelbergh, M., de Prado, M. L., Gómez, E., Llorca, D. F., Herrera-Viedma, E., & Herrera, F. (2025). Aligning trustworthy AI with democracy: A dual taxonomy of opportunities and risks. *arXiv preprint arXiv:2505.13565*.

Milan, S. (2015). From social movements to cloud protesting: the evolution of collective identity. *Information Communication & Society*, *18*(8), 887–900.

Mohamed, S., Png, M., & Isaac, W. (2020). Decolonial AI: Decolonial theory as sociotechnical foresight in artificial intelligence. *Philosophy & Technology*, *33*(4), 659–684.

Mora, F. A. (2014). Emergent digital activism: The generational/technological connection. *Journal of Community Informatics*, *10*(1), 1–13.

Nguyen, C. T. (2020). Echo chambers and epistemic bubbles. *Episteme*, *17*(2), 141–161.

Noble, S. U. (2018). *Algorithms of oppression: How search engines reinforce racism*. New York University Press.

Nurik, C. L. (2022). Facebook and the surveillance assemblage: Policing Black Lives Matter activists & suppressing dissent. *Surveillance & Society*, *20*(1), 30–46.

Overton, S. (2025). Overcoming racial harms to democracy from artificial intelligence. *Iowa Law Review*, 110, 805–866.

Özkula, S. M. (2021a). The unmaking of collective action: Changing organizing logics in civil society organizations through social media activism culture. *International Journal of Communication*, *15* (19), 1984–2002.

Özkula, S. M. (2021b). The problem of history in digital activism: Ideological narratives in digital activism literature. *Journal of Digital Social Research,* 3(3), 60–84.

Özkula, S. M. (2021c). What is digital activism anyway? Social constructions of the 'digital' in contemporary activism. *Journal of Digital Social Research*, *3*(3), 60–84.

Putnam, R. D. (1995). Bowling alone: America's declining social capital. *Journal of Democracy*, *6*(1), 65–78.

Rini, R. (2020). Deepfakes and the epistemic backstop. *Philosophers' Imprint*, *20*(24), 1–16.

Schick, N. (2020). *Deep fakes and the infocalypse*. Octopus Books.

Selbst, A. D., Andrew, L., & Narayanan, A. (2019). Fairness in machine learning: A survey. *Communications of the ACM*, *62*(2), 56–65.

Sloane, M., Moss, E., Awomolo, O., & Forlano, L. (2020). Participation is not a design fix for machine learning. *arXiv.org*, https://doi.org/10.1145/3551624.3555285.

Smith, R. C., Bossen, C., & Kanstrup, A. M. (2017). Participatory design in an era of participation. *CoDesign*, *13*(2), 65–69.

Spielkamp, M. (2017). AlgorithmWatch: What role can a watchdog organization play in ensuring algorithmic accountability? *Transparent Data Mining for Big and Small Data*, 32, 207–215.

Stamboliev, E. (2023). Proposing a postcritical AI literacy: Why we should worry less about algorithmic transparency and more about citizen empowerment. *Media Theory*, *7*(1), 202–232.

Stark, B., Stegmann, D., Magin, M., & Jürgens, P. (2020). Are algorithms a threat to democracy? The rise of intermediaries: A challenge for public discourse. *AlgorithmWatch*, *26*, https://algorithmwatch.org/en/wp-content/uploads/2020/05/Governing-Platforms-communications-study-Stark-May-2020-AlgorithmWatch.pdf.

Suchman, L. (2002). Located accountabilities in technology production. *Scandinavian Journal of Information Systems*, *14*(2), 91–105.

Tsai, L., & Pentland, A. (2025). Rediscovering the pleasures of pluralism: The potential of digitally mediated civic participation. *UCLA Journal of Law and Technology*, 30, 179–195.

Westerlund, M. (2019). The emergence of deepfake technology: A review. *Technology Innovation Management Review*, *9*(11), 40–53.

Zytko, D., Wisniewski, P., Guha, S., Baumer, E., & Lee, M. (2022). Participatory Design of AI Systems: Opportunities and Challenges Across Diverse Users, Relationships, and Application Domains. *Conference: CHI '22: CHI Conference on Human Factors in Computing Systems,* 154, 1–4. https://doi.org/10.1145/3491101.3516506.

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

sciendo

DOI: 10.15290/bsp.2026.31.01.06

Received: 30.06.2025
Accepted: 08.01.2026

Mateja Rek
School of Advanced Social Studies, Nova Gorica, Slovenia
mateja.rek@fuds.si
ORCID ID: 0000–0003–0928–1163

Tea Golob
Faculty of Information Studies, Novo Mesto, Slovenia
tea.golob@fis.unm.si
ORCID ID: 0000–0003–4314–3231

Matej Makarovič
Faculty of Information Studies, Novo Mesto, Slovenia
matej.makarovic@fis.unm.si
ORCID ID: 0000–0001–7864–4285

The Increased Likelihood of Identification as EU Citizens among Critical Yet Positively Minded Young Digital Users

Abstract: In this article, we provide empirical evidence demonstrating that both identification with EU citizenship as well as active digital engagement depend significantly on young people's abilities as critical thinkers. More specifically, we demonstrate that critical yet positively minded young people are more likely to identify as EU citizens. Such healthy sceptics are also more likely to report that they know their citizens' rights and obligations and claim to be well informed about EU decision-making. We provide a more detailed analysis by distinguishing between four categories of youth digital users based on variety in their critical thinking modes and their identification as EU citizens; they can be described as rejecting, engaged, trusting or disinterested. They vary in their level of digital media use, modes of critical thinking, fact-checking and EU identification. We offer evidence indicating that the category of engaged youth demonstrates digital literacy traits that contribute to fostering digital citizenship. In other categories, there is ample opportunity for the enhancement of digital literacy skills. We offer empirically based guidelines tailored to the unique needs of the different groups of youth digital users that we have identified.

Keywords: digital citizenship, EU citizens, youth, critical thinking, digital literacy, e-governance

Introduction

Being an EU citizen means having the nationality of one of the Member States of the European Union. It is associated with several rights and privileges granted by EU law, including freedom of movement, voting rights, consular protection, access to social benefits and consumer rights. EU citizenship complements national citizenship and does not replace it; it offers individuals additional rights and opportunities within the EU and promotes a sense of European identity, unity between citizens and participation in the EU's democratic processes (Adams, 2006; Golob et al., 2024; Mazur & Ramiro Troitiño, 2024; Ramiro Troitiño & Mazur, 2024). But there is more to EU citizenship than just rights: EU citizens are expected to respect the laws and values of the EU, participate in democratic processes and contribute to the common good of society. They are encouraged to inform themselves about society and public affairs and to actively participate in shaping EU policy. EU citizenship fosters a sense of belonging by promoting mobility, political participation, shared values, cultural exchange, social and economic integration, and solidarity among citizens. These multifaceted approaches help individuals feel connected to a larger European community, enhancing their sense of identity and belonging.

Digitalisation significantly impacts the processes related to EU citizenship and the feeling of belonging by enhancing connectivity and participation (Rek, 2024). In the digital age, citizenship straddles both offline and online worlds, referred to as 'real life' and 'immersive reality'. It is claimed that regardless of the extent of convergence between the physical and virtual worlds, citizens must be digitally competent to be active citizens (Costa, 2023; Frau-Meigs et al., 2017 Mokrá, 2023; Rūse, 2014). A key element of digital citizenship identified in many definitions is the notion of digital engagement, brought about by the competent use of digital technology (González-Cacheda & Outeda, 2021; Kerikmäe et al., 2019; Outeda, 2024; Ramiro Troitiño et al., 2023). The specific know-how or skills required for digital citizenship are also frequently referred to in the literature.

At the heart of e-democracy lies the concept of media literacy, an indispensable skill set that empowers citizens to critically engage with digital media and navigate the complexities of the information age (Ayata, 2024; Buckingham & Sefton-Green, 2018; Hobbs, 2010; Livingstone, 2004). Media literacy encompasses the ability to access, analyse, evaluate and create media content in various formats, from traditional news outlets to social media platforms. In the context of e-democracy, it plays a transformative role in fostering informed citizenship, combating misinformation and promoting a vibrant public discourse (Giovanola, 2023; Hamuľák, 2016; Maatsch, 2024; Martens, 2015). Critical thinking is a core element of media literacy; it is the ability of individuals to use and at the same time autonomously and critically interpret the flow, content, values and consequences of the use of various media messages (Ferretti, 2022). It also enables them to participate in the creation of media messages (Golob

et al., 2021; Martens, 2015). Improving critical thinking and digital media literacy has thus become of strategic importance for active citizenship in the EU (European Commission, 2018, p. 25).

A digital citizen is someone who, through the development of a broad range of competences, is able to actively, positively and responsibly engage in both on – and offline communities, at the local, national or transnational levels. As digital technologies are disruptive in nature and constantly evolving, building competence is a lifelong process that should begin from earliest childhood at home and at school, in formal, informal and non-formal educational settings (Richardson & Milovidov, 2019). The Council of Europe has been very active in fostering digital citizenship in the EU by promoting digital citizenship education. Our children and young people are our future, and they spend a lot of time nowadays connected to digital media. To communicate, learn, work and play responsibly in this environment, they need to develop a whole range of media literacy competences that will enable them to take advantage of benefits and opportunities and overcome the pitfalls they will encounter. Young people today are in the vanguard of new media practices (Sarrica et al., 2010), so equipping them with critical digital and media literacy skills is essential for them to navigate the online public sphere and make informed decisions as citizens (Bečević & Dahlstedt, 2022). Rapid social change and the unprecedented exposure of children and young people to digital media imply that digital media education cannot rely solely on obtained information and/or pre-given norms; instead, reflexive deliberations on the ongoing challenges brought forwards by social complexity and dynamics are needed (Golob et al., 2023).

In this article, we present the results of a survey that was carried out in 2024 on a nationally representative sample of high-school students in Slovenia, exploring their digital media habits and certain elements of media literacy (Rek, 2024). In addition to reporting on their own media habits and issues related to such use, the students were asked if they feel as if they are European citizens and how well informed they are about political decision-making in the EU. We explore whether identification with EU citizenship and active digital engagement is related to young people's digital media habits. We speculate on whether young critical thinkers are more likely to identify as EU citizens, and we look for consistent patterns of digital media use as well as critical thinking which could explain the diversity in their identification as EU citizens and differences in their levels of information about political decision-making in the EU (de la Guardia, 2005).

The central objective is to identify the key categories of young people in terms of their feelings of EU citizenship and their patterns of using digital media, while attempting to understand them in a broader context. This way, potential target groups for future policies can be identified. Our basic assumption is that active EU citizenship requires both identification with EU citizenship and competent digital media practices that involve critical fact-checking. We believe that our research can contrib-

ute to future efforts in digital citizenship education by providing a nuanced understanding of young people's feelings of EU citizenship. There is a lot of diversity in the way children and young people use digital media, and our research enables an understanding of this diversity and its impact on the sense of EU citizenship they have. By leveraging these insights, we can better equip young people with the critical thinking skills, media literacy and sense of EU identity necessary to thrive in an increasingly digital and interconnected world.

1. Materials and methods

In empirical terms, our research is primarily based on a survey conducted on a representative sample of 2,314 high-school students in Slovenia that took place from 13 February to 13 April 2024, as a part of longitudinal studies on media literacy and digital practices within the Infrastructure Programme in Media Literacy in Slovenia supported by the Slovenian Research and Innovation Agency (Rek et al., 2024). The survey questionnaire and its implementation were designed in a way to maximise the response rate and minimise response biases and missing values. For these purposes, the survey was tested through a pilot. The analyses revealed no biases or inconsistencies that could affect overall validity.

Within the survey questionnaire we focused on the relationship between, on the one hand, feelings of European Union citizenship in a more classical sense, and on the other, competences and behaviours in the digital realm as a bridge to digital European citizenship. A classical commitment to European citizenship, a feeling of belonging to the European demos, is approximated through a five-level Likert scale measuring agreement with the statements 'I feel like a citizen of the European Union' and 'I am well informed about political decision-making in the European Union'. The ways in which the high-school students are able to manage digital (public) spaces was assessed through a combination of four questions that combined doubting and checking the content found on social networks and on web information portals through a five-level Likert scale ranging from 'never' to 'always', namely:

- 'How often do you doubt the information you have found on social networks?'
- 'How often do you doubt the information you have found on web information portals?'
- 'How often do you additionally check the information you have found on social networks with another source?'
- 'How often do you additionally check the information you have found on web information portals with another source?'

This way, not only the critical but also the active stances taken in the digital space can be observed.

While the combinations of answers to these six questions may lead to a rather complex variety of views and behaviours, we have enabled a more systematic and straightforward analysis by distinguishing between different categories of high-school students based on the responses to these questions. K-means clustering based on Euclidean distances has been applied for this purpose, including the six above-mentioned variables as criteria to define the clusters.

The most concise yet still sufficiently nuanced solution suitable for meaningful interpretation consists of four clusters. In this way the model can provide two-by-two combinations between the two major conceptual dimensions: patterns of digital media use and attitudes towards the EU. We have analysed and compared them to each other in terms of basic demographic features, current position in the educational system, digital and media habits, and some general attitudes towards life. The demographic variables include the respondent's gender, age and whether they are living in shared custody (implying that their parents have separated or divorced). Within the education section, we distinguish between general secondary education (typically a gymnasium finishing with a general Matura exam) and vocational secondary education (typically finishing with a vocational Matura consisting of a smaller number of subjects). We also asked them whether they were planning to continue their studies after finishing secondary education and about their previous year's achievement in terms of their average grade.

Regarding their digital behaviour and media habits in general, we asked them to report their frequency of watching TV, videos or movies (recorded or live), listening to the radio, using a computer or tablet for any purpose, using a mobile phone for any purpose, listening to music, reading magazines, newspapers and other printed media in a paper form, playing video games (on any platform), playing video games with violent content (shooting, fighting and similar), using a computer or tablet for learning or other work, being present in a room where a TV is on, and being present on social networks (Facebook, X, Instagram, Pinterest, TikTok, etc.). They were also asked to report their level of agreement on the five-level Likert scale with statements about regularly following information content in the Slovenian or foreign media.

General features and attitudes towards life were observed in terms of agreement with the following statements (on five-level Likert scales): 'My health is excellent'; 'My life is empty and meaningless for me'; 'I am satisfied with the course of my life'. For the purposes of our analyses, Likert-scale variables were considered as interval ones, enabling us to apply a broader range of statistical methods and tests. A chi-square test was applied while comparing categorical (nominal) variables and analyses of variance tests checked the relationships between categorical and interval variables. A Scheffé test was applied to test the significance levels of differences between the categories.

2. Results

The identification of the high-school students included in our sample with the EU is rather high, with 26.8% fully agreeing and another 19% agreeing with the statement that they feel citizens of the European Union. Only 10.6% claimed that they strongly disagree. However, they mostly do not feel well informed about the political decision-making in the EU: a clear majority of 54.8% disagreed or strongly disagreed, while only 5.5% fully agreed that they are well informed about it.

Regarding information found on social networks, they are quite doubtful: 14.5% always doubts it, while only 5.5% never doubts. The majority leans towards moderate doubt, with 38.8% choosing the middle value of 3, and 29.6% expressing somewhat higher doubts with the value of 4. There is less doubt about online information portals, with 7.1% never doubting them and 9.3% always doubting them. Almost half – 48% – chose the middle value. Nevertheless, while those who doubt are also more likely to check, doubt does not always lead to checking the information with another source. Only 9.4% of respondents always check social network content, and only 6.8% always checks information portals' content, with another 19.7% and 13.5% respectively mostly doing this (the value of 4 on the five-level scale). 17.8% of respondents never check social networks' content with another source, and 24.6% never do this for the online information portals.

The clusters identified through the k-means clustering of these six variables are presented in Table 1. Comparatively the largest cluster (38.2% of respondents) expresses strong feelings of EU citizenship and also feels rather well informed about political decision-making in the EU. On the other hand, they are below average when it comes to frequency of doubting or checking digital content. While they feel informed as citizens, they gladly accept digital content without major doubts. We may see trust as their key feature in this regard, so they can be called trusters.

Table 1. Differences from the overall mean for the identified clusters.

Variables Clusters	Feels like an EU citizen	Well informed about EU decision-making	Doubts information on social networks	Doubts information on online information portals	Checks information on social networks	Checks information on online information portals
Detachers	-0.84	-0.55	-0.97	-0.88	-1.28	-1.25
Trusters	0.77	0.36	-0.15	-0.11	-0.34	-0.33
Engagers	0.81	0.56	0.77	0.71	1.31	1.36
Rejectors	-1.13	-0.53	0.37	0.30	0.49	0.42
Overall mean	**3.44**	**2.41**	**3.36**	**3.09**	**2.87**	**2.60**

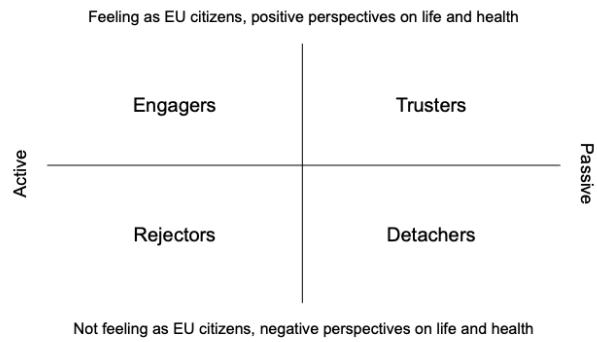
Source: Own calculations

The second biggest group (25.6%) is their direct opposite. They strongly reject feelings of EU citizenship, do not consider themselves well informed about EU political decision-making and are above average when it comes to doubting and checking information published on social networks and web information portals. They seem to be characterised by serious doubts or even rejection when it comes either to identifying with the EU and its politics or to using digital spaces. They can thus be denoted as rejectors.

The third group (18.2% of the respondents) also tends not to feel like EU citizens and not to be well informed about EU political decisions. On the other hand, they seem to rather blindly accept the information they find on social networks and online information portals, as they are the least likely to doubt or check the information in digital spaces, when compared to the other clusters. As they seem mostly detached from the EU and its politics, while also not being interested in taking a more active stance in digital public spaces, they can be called detachers.

The final group, of roughly the same size (18% of respondents), can be seen as their direct opposite. They have strong feelings of EU citizenship and feel well informed about its political decision-making. They are more likely than any other category to doubt and check digital content – even more than the rejectors' cluster. They seem to be the category that is comparatively most actively engaged as EU citizens, both in terms of classical and digital citizenship, as they seem to follow political news about the EU, while also being capable of engaging in digital public spaces, demonstrating not just a healthy scepticism but also conscientious checking of digital content. We can therefore denote them as engagers. The four groups and their key differences through the two major dimensions are summarised in Figure 1.

Figure 1. Statistically significant differences between the clusters.



Source: Authors' own elaboration

In Table 2 we provide a more detailed overview of the differences between the four clusters in terms of basic demography, position in the educational system, digital and other media habits, and some perspectives about life that have turned out to be statistically significant. While the differences between genders are not major, they are statistically significant. There are slightly fewer engagers and slightly more rejectors among women. Those who declared themselves as non-binary are slightly more likely to be detachers and rejectors and less likely to be trusters or engagers. It also seems that the share of trusters declines and the share of detachers increases as the students get older. Living in shared custody, on the other hand, demonstrated no statistically significant effect on belonging to any of these categories.

Table 2. Statistically significant differences between the clusters.

		Detachers	**Trusters**	**Engagers**	**Rejectors**	**Statistical test applied***
Demography	Gender	Non-binary	Less among other	Less among women	More among women and other	Chi-square (0.002)
	Age	More among older	More among younger			Scheffé (0.018)
Education	High-school type		More in vocational education	More in general education		Chi-square (0.012)
	Plans for further education	Less likely to continue studying		More likely to continue studying		Chi-square (0.000)
	Average grade	Lower than trusters and engagers	Higher than detachers (0.008)	Higher than detachers (0.001)		Scheffé
Media habits	Using computer or tablet		Less often	More often		Scheffé (0.052)
	Using mobile phone	More often	Less often			Scheffé (0.010)
	Reading printed media		Less often	More often		Scheffé (0.012)
	Using computer or tablet for study or other work	Less often than engagers (0.010)	Less often than engagers (0.000)	More often than detachers and trusters		Scheffé
	Present when TV on	More often than trusters and rejectors	Less often than detachers (0.009)		Less often than detachers (0.048)	Scheffé
	Presence in social networks	More often	Less often			Scheffé (0.036)
	Following information content in Slovenian media	Less often than all	More often than detachers (0.000) and rejectors (0.000)	More often than all	More often than detachers (0.002)	Scheffé

	Following information content in foreign media	Less often than all	More often than detachers (0.000) and rejectors (0.020)	More often than all	More often than detachers (0.001)	Scheffé
Perspectives about life	Reported health	Worse	Better	Better	Worse	Scheffé (0.000)
	Seeing life as empty and meaningless		Less likely		More likely	Scheffé (0.021)
	Satisfied with course of life	Less than trusters and engagers	More than detachers (0.000) and rejectors (0.000)	More than detachers (0.002) and rejectors (0.008)	Less than trusters and engagers	Scheffé

** Statistical tests are provided with significance levels in brackets. When differences are detected between more than two different groups, significance levels are provided separately under each group.*

While trusters are slightly more common in vocational high schools, engagers are more frequent in the general education high schools. Engagers are more likely than detachers to continue their studies after high school, according to their own claims. On top of that, detachers have statistically significant lower educational performance in terms of average grades when compared to trusters and engagers.

Trusters are the least frequent users of the media, both digital and traditional, especially when compared to the engagers. They use computers or tablets and mobile phones less often, and they are less present in online social networks; they are less likely to be exposed to the TV and less likely to read classical printed media. On the other hand, despite the comparatively lower frequency of their media practices, they are far from being totally excluded from following the news, as they are more likely to report following the information content of Slovenian and foreign media when compared to rejectors and detachers.

Engagers, on the other hand, seem to be the most frequent users of computers or tablets, both in general when compared to trusters and for educational and other work purposes when compared to trusters and detachers. Heavy use of digital media in their case, however, does not mean ignoring the traditional media, as they also report more frequent use of printed media. Consistently with that, they also report following the information content in Slovenian and foreign media to a higher extent than any other group.

Detachers are also quite heavy users of digital media, but their patterns of use are rather different from those of the engagers. Detachers use their smartphones and are present on social networks more frequently than trusters. They are more exposed to TV screens than trusters and rejectors. However, they are less likely than engagers to use computers or tablets for study or other work. Among all categories, they report the lowest following of information content in Slovenian and foreign media.

Finally, the rejectors do not stand out in most of the digital and classical media behaviours, being typically in between when compared to the behaviours of other

groups. They are not excessive media consumers, but they are also far from being excluded from the digital or offline media spaces. They are less often exposed to turned-on TV screens when compared to detachers, but are also more likely than them to follow information content in Slovenian and foreign media.

The four clusters also differ from each other in terms of perceptions of their lives. Trusters and engagers report significantly better health than rejectors and detachers. Rejectors are more likely to see their lives as empty and meaningless when compared to trusters. On top of that, engagers and trusters report significantly higher satisfaction with their lives than rejectors and detachers.

Conclusions

The clustering of high-school students into the four clusters provides a truly valuable tool, both for a better understanding of predispositions and challenges for digital EU citizenship and as a starting point for further research and the development of policy recommendations in this field. The cluster denoted as engagers is clearly the closest to a normative ideal of an active European digital citizen. They feel like EU citizens, competently and extensively navigate digital spaces, extensively use digital tools and keep themselves informed from a variety of media ranging from the classical to the digital. Their healthy scepticism towards media content combined with a readiness to check the media content with other sources makes them least vulnerable to extremist perspectives, fake news and political or other manipulation.

On the other hand, detachers seem to be the most vulnerable category in this regard, especially because of their lack of doubting and checking digital content, combined with their detachment from EU politics and established information sources. Like engagers, they are heavily involved with digital technologies, but they follow clearly different patterns: more smartphones instead of computers, more social media instead of information media (perhaps mostly obtaining information from social networks instead of the established media) and a lower ability and/or readiness to exploit digital technologies for study and work.

Although the trusters share their trust in digital content with the detachers, they are less directly vulnerable than the latter because their online presence is more moderate and they are more open to a variety of information sources. However, as they are typically slightly younger, one may at least partly see them as a transitional category that may develop either towards becoming engagers if they establish a more mature attitude towards digital content, or towards becoming detachers if they become disappointed by political and/or other developments. This could become a very relevant topic for future research, especially in longitudinal terms.

Finally, while the rejectors do not feel very close to the EU, they do possess some features that could make them active digital citizens. They do not seem to be exces-

sively exposed to the most harmful digital media practices, and they share at least some inclination to doubt and check digital media content with the trusters. Some of their critical attitudes may even become a positive source for change – for themselves and for society. On the other hand, if some of their more questionable features prevail, such as their pessimism about life and lack of interest in politics and in established information sources, they may become closer to the detachers, and also a vulnerable target for fake news, conspiracy theories and other forms of manipulation. Again, these kinds of potential transformation would be a very relevant research topic with significant policy implications.

While observing these four categories, we should pay particular attention to the problem of social inequalities. Different positions in the social structure may strongly affect to which cluster an individual belongs. Trusters and engagers are healthier and happier than detachers and rejectors. While this may be a result of fully subjective psychological features, it may also result from the objective factors to which individuals have been exposed – including a variety of possible social deprivations. We should also be aware that the educational system is not fully meritocratic, so the differences in plans for further education and the educational achievements in terms of grades are not just a result of individuals' hard work, creativity and other competences, but also of their social backgrounds.

The gender issues should also not be neglected in this regard, though the differences are slight. Active digital citizenship as represented by the engagers seems to be slightly more accessible to young men than to young women. It may also be indicative that detachers and rejectors are slightly more common among those who reported their gender as 'other'; this may reflect some problems with social exclusion facing non-binary youth. While it is also possible that some of the students choosing this category were not fully serious about it (and would otherwise define as either men or women), it would still demonstrate a particular attitude towards dealing with the questionnaire used in our survey – perhaps indicating some form of detachment, self-exclusion and/or protest. These may again be compatible with the digital practices of detachers and rejectors.

The results we obtained show that young people vary widely in terms of their digital practices, perspectives on life and social embeddedness that impact their identifications with EU citizenship. This variety should be of great importance for the EU when developing and implementing policies related to different areas within education, media literacy, digitalisation skills and civic engagement. On that basis, we suggest three different pillars of recommendations, emphasising general policy orientation and simultaneously embracing the diversity of the young population in the EU.

1. Enhancing general knowledge about EU citizenship

Firstly, it is important to invest in the general knowledge about democratic practices and the advantages of political participation. Young people, who represent the

pillars of our future society, should be well informed about their rights as EU citizens. It is important to expand citizenship education in a formal context and upgrade the existing curricula, but simultaneously also in more informal ways through different events, platforms and activities that bring young people together. Such actions are especially relevant for the rejectors group, who are not only strongly present online but also critically check media content and doubt information, while they express a low level of being informed about EU decision-making. They should be encouraged to utilise their digital skills for enhancing their digital citizenship practices for strengthening democracy in the EU.

Increasing general knowledge about the EU and citizenship is also fundamental for the trusters group, which is the youngest. Steered education about EU citizenship and democracy could contribute to enhancing their potential to become engagers. Educational activities are also important for the detachers group, where a lack of knowledge is combined with overall passivity in media fact-checking and related media literacy.

2. Boosting competences for digital citizenship

This brings us to the second pillar of recommendations, which emphasise that the general European citizenship skills should be combined with digital platform competences. The European legal framework increasingly expects both platform operators and users to understand and engage with transparency and data-sharing mechanisms that underpin digital participation within the EU (Nyka & Zapolska, 2024). Youth from all four clusters are to be approached as active agents who can contribute to the meaning and practice of citizenship itself. For that purpose, the establishment of digital platforms where they can exchange their concerns and ideas seems crucial. Campaigns such as the European Citizens' Initiative, based on a digital platform, allow citizens to propose legislation, and such digital platforms can feed into a more targeted youth platform. Young people should be encouraged to express their creativity, needs and expectations in conceiving EU policies (Sime & Behrens, 2023 and the role of citizens in implementing them. Such initiatives should be provided from local to EU levels, thus presenting a key to fostering a sense of belonging to the European Union (Bečević & Dahlstedt, 2022).

Creating a proper infrastructure is a necessary condition to boost identification with EU citizenship; however, the skills for using it are equally important. Youth from all four clusters should be equipped with the knowledge and skills to enable the EU to fully harness the potential of digital tools to empower its citizens. Policymakers should invest more in digital competence education to foster digital literacy, which is especially important in the context of detachers and trusters. For engagers and rejectors, those initiatives could contribute to bridging the gap between citizens' digital skills and their declining faith in media.

3. Strengthening trust in media content about the EU

Thirdly, as the EU works to strengthen its digital identity and online services, it should also address the issue of disinformation and invest heavily in combating the corrosive effects of fake news and echo chambers arising in social media (Kiratli, 2023). At the same time, this process must be accompanied by a strong commitment to privacy protection and the ethical use of personal data, recognising the growing risks of profiling and data misuse in the digital sphere (Kuźnicka-Błaszkowska & Jabloński, 2024; Rejmaniak, 2021). These activities are especially important for the detachers group, and to a certain extent for the trusters, who are strongly present on social media but rarely check the content source or doubt the information. They are most vulnerable to fake news and harmful propaganda that undermines the basis of EU democracy. The EU should provide more active implementation of strategies and activities, such as EUvsDisinfo, which directly target the young population. The latter is crucial to combatting the spread of information that is demolishing the legitimacy and reputation of the EU as a political entity that safeguards citizens' rights and assures economic prosperity and sustainability. In addition, the EU should invest in promoting itself widely through social media, as these are the only information channels that the detachers group is following. Regardless of the variety within the youth clusters, the EU should strengthen its transparency and accountability through regular updates from EU bodies via their official websites and social media. It should provide accurate information and expose false narratives to enhance trust in digital media sources.

REFERENCES

Adams, M. (2006). Hybridizing habitus and reflexivity: Towards an understanding of contemporary identity? *Sociology*, *40*(3), 511–528.

Ayata, Z. (2024). European Union contracts in digital environments. In D. Ramiro Troitiño (Ed.), *E-governance in the European Union: Strategies, tools, and implementation* (pp. 173–185). Springer Nature Switzerland.

Bečević, Z., & Dahlstedt, M. (2022). On the margins of citizenship: Youth participation and youth exclusion in times of neoliberal urbanism. *Journal of Youth Studies*, *25*(3), 362–379.

Buckingham, D., & Sefton-Green, J. (2018). Multimedia education: Media literacy in the age of digital culture. In R. Kubey (Ed.), *Media literacy around the world* (pp. 285–305). Routledge.

Costa, M. I. (2023). The legal concept of discrimination by association: Where does it fit into the digital era? *UNIO–EU Law Journal*, *9*(1), 16–28.

de la Guardia, R. M. (2005). La política europea de España después de su integración en las Comunidades. *Cuadernos europeos de Deusto*, *32*, 61–84.

European Commission. (2018). The multi-dimensional approach to disinformation: Report of the Independent and High Level Group on Fake News and Online Disinformation. Directorate-General for Communication

Networks, Content and Technology. Available at: file:///C:/Users/rekma/Downloads/a%20multi-dimensional%20approach%20to%20disinformation-KK0118221ENN.pdf

Ferretti, F. (2022). A single European data space and data act for the digital single market: On datafication and the viability of a PSD2-like access regime for the platform economy. *European Journal of Legal Studies*, *14*, 173–218.

Frau-Meigs, D., O'Neill, B., Soriani, A., & Tomé, V. (2017). *Digital citizenship education: Vol. 1. Overview and new perspectives*. Council of Europe.

Giovanola, B. (2023). Justice, emotions, socially disruptive technologies. *Critical Review of International Social and Political Philosophy*, *26*(1), 104–119.

Golob, T., Makarovič, M., & Rek, M. (2021). Meta-reflexividad para la resiliencia contra la desinformación. *Comunicar: Revista Científica de Comunicación y Educación*, *66*, 107–118.

Golob, T., Makarovič, M., & Rek, M. (2023). Parents' meta-reflexivity benefits media education of children. *Comunicar: Media Education Research Journal*, *31*(76), 95–103.

Golob, T., Rek, M., & Makarovič, M. (2024). European citizenship and digitalization: A new roadmap for interconnection. *Internet of things*, *27*, 101282.

González-Cacheda, B., & Outeda, C. C. (2021). Political crowdfunding and resource mobilization for collective action: The keys to success. *Technology in Society*, *67*, 101743.

Hamuľák, O. (2016). *National sovereignty in the European Union: View from the Czech perspective*. Springer.

Hobbs, R. (2010). *Digital and media literacy: A plan of action. A White Paper on the digital and media literacy recommendations of the Knight Commission on the information needs of communities in a democracy*. Aspen Institute.

Kerikmäe, T., Ramiro Troitiño, D., & Shumilo, O. (2019). An idol or an ideal? A case study of Estonian e-governance: Public perceptions, myths and misbeliefs. *Acta Baltica Historiae et Philosophiae Scientiarum*, *7*(1), 71–80.

Kiratli, O. S. (2023). Social media effects on public trust in the European Union. *Public Opinion Quarterly*, *87*(3), 749–763.

Kuźnicka-Błaszkowska, D., & Jabloński, M. (2024). Information on gender identity as personal data under EU and US data protection models. *Białostockie Studia Prawnicze*, *29*(3), 207–220.

Livingstone, S. (2004). Media literacy and the challenge of new information and communication technologies. *The Communication Review*, *7*(1), 3–14.

Maatsch, A. (2024). Parliamentary adjustment during a crisis: Interplay of digitalization and domestic context factors. *Internet of Things*, *27*, 101316.

Martens, H., & Hobbs, R. (2015). How media literacy supports civic engagement in a digital age. *Atlantic Journal of Communication*, *23*(2), 120–137.

Mazur, V., & Ramiro Troitiño, D. (2024). The members of the EU and e-governance, analysis, and institutional support. In D. Ramiro Troitiño (Ed.), *E-governance in the European Union: Strategies, tools, and implementation* (pp. 39–55). Springer Nature Switzerland.

Mokrá, L. (2023). Digitally sovereign individuals: The right to disconnect as a new challenge for European legislation in the context of building the EU digital market. In D. Ramiro Troitiño, T. Ker-

ikmäe, & O. Hamuľák (Eds.), *Digital development of the European Union: An interdisciplinary perspective* (pp. 189–197). Springer International Publishing.

Nyka, M., & Zapolska, K. (2024). The impact of the DAC7 Directive on the functioning of platforms and platform operators. *Bialystok Legal Studies*, *29*(2), 177–193.

Outeda, C. C. (2024). The EU's AI Act: A framework for collaborative governance. *Internet of Things*, *27*(3) 101291.

Ramiro Troitiño, D., & Mazur, V. (2024). E-identity: A step forward to European digital citizenship. In D. Ramiro Troitiño (Ed.), *E-governance in the European Union: Strategies, tools, and implementation* (pp. 57–70). Springer Nature Switzerland.

Ramiro Troitiño, D., Kerikmäe, T., & Hamuľák, O. (2023). The digital future of the European Union. In D. Ramiro Troitiño, T. Kerikmäe, & O. Hamuľák (Eds.), *Digital development of the European Union: An interdiscipinary perspective* (pp. 3–6). Springer.

Rejmaniak, R. (2021). Bias in artificial intelligence systems. *Białostockie Studia Prawnicze*, *26*(3), 25–44.

Rek, M. (2024). E-democracy in the EU. In D. Ramiro Troitiño (Ed.), *E-governance in the European Union: Strategies, tools, and implementation* (pp. 103–115). Springer Nature Switzerland.

Rek, M., Ljubotina, P., & Bašin, A. (2024). *Media and high school students in Slovenia*. Infrastructure Programme Media Literacy in Slovenia. Available at: https://zenodo.org/records/18265813

Richardson, J., & Milovidov, E. (2019). *Digital citizenship education handbook: Being online, well-being online, and rights online*. Council of Europe.

Rūse, I. (2014). Nordic–Baltic interaction in European Union negotiations: Taking advantage of institutionalized cooperation. *Journal of Baltic Studies*, *45*(2), 229–246.

Sarrica, M., Grimaldi, F., & Nencini, A. (2010). Youth, citizenship and media: An exploration from the social representations perspective. *Revue internationale de psychologie sociale*, *23*(4), 37–62.

Sime, D., & Behrens, S. (2023). Marginalized (non)citizens: Migrant youth political engagement, volunteering and performative citizenship in the context of Brexit. *Ethnic and Racial Studies*, *46*(7), 1502–1526.

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

sciendo

DOI: 10.15290/bsp.2026.31.01.07

Received: 09.06.2025
Accepted: 03.03.2026

Karolina Kiejnich-Kruk
Adam Mickiewicz University, Poland
kiejnich-kruk@amu.edu.pl
ORCID ID: 0000–0003–1551–5448

The AI Act: Challenges for Justice and Democracy in the Deployment of AI-Based Systems

Abstract: The entry into force of the AI Act will have a significant impact on the practices of both private and public actors. The Act identifies areas where there is a particularly high risk of the violation of fundamental rights, including the administration of justice and democratic processes. This article analyses the provisions of the AI Act for the use of AI systems in these areas, outlines the framework for their use and identifies the main risks to human rights. It considers the most important challenges arising from the AI Act in relation to justice and democratic processes, as well as the difficulties in interpreting the Act in this regard. It also proposes an approach that EU Member States can follow to adjust their national legal systems to meet these new challenges. It suggests that these challenges require a coherent process for the digitisation of justice that distinguishes between systems subject to high-risk AI regulation and those that can be implemented without such burdens. Regarding democratic processes, Member States must implement regulations that, first, promote transparency in the use of AI tools and, second, encourage cooperation with online platforms in monitoring them.

Keywords: AI Act, administration of justice, democratic processes, elections, artificial intelligence

Introduction

The Artificial Intelligence Act (the AI Act or the Regulation) (European Parliament and the Council, 2024) marks a significant milestone in the legal regulation of artificial intelligence systems in various social and economic sectors. It has a significant impact on both the private and the public sectors, including in relation to the administration of justice and democratic processes. Of particular relevance in this regard are its regulations concerning high-risk AI systems; the Act identifies these

areas as being particularly likely to give rise to human rights violations due to the use of AI technologies. Classifying a particular system into the appropriate category – prohibited, high-risk or not subject to these regimes – is crucial for the proper implementation and use of such a system. This is particularly important for safeguarding the fundamental rights of participants in the legal proceedings by implementing the right controls and minimising risks. Additionally, misclassifying a system may result in actors in the supply chain failing to comply with the obligations set out in the Regulation, which could lead to sanctions.

This article aims to analyse the provisions of the AI Act regarding the use of AI systems within the areas of the administration of justice and democratic processes, in order to outline the framework for their use and to detect the main risks to human rights arising from them. The paper presents an analysis of the most important challenges arising from the AI Act in the areas of justice and democratic processes, the difficulties in interpreting the Regulation in this regard, and the guidelines for EU Member States on possible policy directions for adapting their national legal frameworks to the identified challenges.

The first subsection of the paper outlines the reasons for categorising the above-mentioned areas as high-risk and the implications of this for public entities using AI systems in these spheres. The second subsection focuses on the administration of justice and considers the interpretation of the provisions of the AI Act in this domain, the challenges associated with the implementation of these provisions and the proposed national approach to emerging challenges. The third subsection provides an analysis of the provisions of the Act relating to democratic processes, the impact of new technologies on electoral processes, the risks involved and proposals for avoiding these risks. It also covers the tools currently available under EU law. The research is based on a formal analysis of the relevant legal norms. It also employs the dogmatic method, with a focus on the national and international literature on both the legal and the technical aspects of the use of AI systems in the areas of justice and elections.

1. High-risk AI systems: Requirements for public actors

A significant number of the AI systems used in the administration of justice and in democratic processes are considered to be high-risk. As indicated in Recital 61 of the Preamble of the AI Act, this is due to their potential impact on the rule of law, personal freedoms and the right to an effective remedy and access to an impartial tribunal. The aim of putting these systems in this category is to eliminate the potential risks of bias, error and the black-box effect (Brożek et al., 2024; Hassija et al., 2024). Therefore, while AI tools can support the independence of the judiciary or judges' decision-making processes, they should not replace them; final decision-making must remain a human-led activity. It is important to note that AI systems should not be

classified as high-risk if they are intended for purely ancillary administrative activities that do not affect the administration of justice in individual cases. Examples include systems used for anonymising or pseudonymising court decisions, documents or data, for communication between staff members and for administrative tasks.

Also, as indicated in Recital 62 of the Preamble, to prevent undue external interference with the right to vote, as well as any undesirable impacts on democracy and the rule of law, AI systems intended for use in influencing election or referendum outcomes or the voting behaviour of individuals should be classified as high-risk. The exceptions are systems which produce results that individuals are not directly exposed to, such as tools used to organise, optimise or structure political campaigns from an administrative or logistical point of view. Direct exposure therefore refers to the rights of individuals, including the right to vote, the right to privacy and the protection of personal data in the context of data analytics used to target media messages.

The legislation combines both the administration of justice and democratic processes into a single legislative unit, due to the same category of rights and values being at risk as a result of AI systems being used in these areas. These can be referred to collectively as 'country governance'. As indicated in the Preamble, the rights and values in question are democracy, the rule of law, individual freedoms and the rights to an effective remedy and to a fair trial.

Putting a system into the high-risk category has significant implications. Such systems occupy a central position in the Regulation; they have been given the most attention, and it has been recognised that they require specific regulation. The broad aim of the Regulation is to monitor, prevent and minimise the impact of AI risks, which apply at all stages of the supply chain, including system design and development, implementation, import, release and use. At the same time, the major responsibilities lie with the providers and deployers of these systems. Given the specificity of the areas in question, the entities responsible for deployment will be public bodies; their main obligations are set out in Articles 26 and 27 of the AI Act.

The purpose of this paper is not to discuss all the obligations in this area, but it is reasonable to point out the most important ones and those that raise the most doubts. Article 26(1–4) imposes the following obligations on entities applying high-risk AI systems:

1) taking technical and organisational measures to monitor the compliance of the operation of the AI system with the user manual;
2) entrusting supervision to natural persons who have the necessary competence, training and authorisation, as well as the necessary support; and
3) to the extent that the entity exercises control over input data, ensuring the adequacy and sufficient representativeness of input data in relation to the intended use of the high-risk AI system.

Technical and organisational measures include, for example, the creation of appropriate procedures in the event of irregularities being detected by any user, regular internal audits to verify compliance with the user manual, regular training for employees and the introduction of automatic alerts in the event of results that deviate significantly from the average. Supervisory duties involve introducing a 'human-on-the-loop' principle rather than the 'human-in-the-loop' principle (Pinto et al., 2013). This means that a human has the role of controlling the operation of the system, not actively interacting with the system, by providing feedback on the correctness of the results as a permanent element of the learning process. At the same time, this supervision must be real, not just apparent; the supervisor must have the appropriate competences, training and authorisation, and must have knowledge and experience in the field of high-risk AI systems, covering applicable standards and existing threats to the violation of those standards, risks of irregularities and proper reactions to the detection of risks. It is desirable for supervisors to be changed on a regular basis, as research shows that individuals tend to become tired or distracted when working with autonomous systems (Weitkunat & Bestle, 1990), so they cannot actively monitor AI systems for long periods without the risk of undetected irregularities increasing. This is also related to a psychological effect, with individuals assuming that these systems cannot fail or 'make a mistake', even though this happens more often than not (Weitkunat & Bestle, 1990).

With regard to input data, the user is required to ensure that the input data is adequate and sufficiently representative for the purpose of the high-risk AI system. 'Input data' refers to the data provided to or directly obtained by the AI system on which the system bases its generation of results (Article 3(33) of the AI Act). Typically, the system's design specifies the input data required to obtain a result.

Article 27 establishes the obligation to conduct an impact assessment on fundamental rights in connection with the implementation of a high-risk AI system. Identifying the risks to fundamental rights is a crucial first step in addressing such risks, for example by enabling the adoption of appropriate mitigation measures. This issue has already been discussed by scholars (Fülöp & Poindl, 2025; Mentelero, 2024), but it seems sensible to point out the most important issues in this regard. The risk assessment should relate to the fundamental rights listed in the AI Act; key rights that may be at risk are identified in Recital 48 of the Preamble. The specific fundamental rights against which the assessment should be conducted depend on the specifics of the operation of the given system and the area in which it is to be used. For example, based on an analysis of selected AI applications in the public sector, the EU Agency for Fundamental Rights (FRA) has identified the specific impact of AI systems on human dignity, the right to privacy and protection of personal data, the right to equality and non-discrimination, the right to an effective remedy and access to an impartial court, the right to social security and social assistance, consumer protection and the right to good administration (FRA, 2020, pp. 57–86). In practice, however, these assessments are often informal. According to the FRA, providers and deployers tend to focus on a

limited number of potentially affected rights, most notably privacy and data protection, and occasionally non-discrimination and access to an effective remedy (FRA, 2025, p. 34). There is little awareness of more specific rights that may be relevant in different sectors. For instance, in the research conducted by the FRA, none of the respondents working in law enforcement mentioned the presumption of innocence or the right to defence (Article 48 of the Charter) (FRA, 2025, p. 36). This suggests that Fundamental Rights Impact Assessments (FRIAs) need to be carried out more effectively, with greater awareness of the full range of fundamental rights that may be affected by AI systems in specific contexts and of how these rights relate to the use of AI. One way to achieve this would be to guide those conducting the assessments towards the rights most likely to be impacted based on the characteristics of the AI system and its deployment context (FRA, 2025, p. 43).

Of particular importance in the context of systems used in the administration of justice and democratic processes is that the risk assessment should indicate specific mechanisms for counteracting threats and ways of responding to their occurrence, as required by Article 27(1)(e) and (f) of the AI Act. It is important that these mechanisms are not only formally established but also have a real impact on detecting and correcting potential errors and on reducing the risk of results being automatically approved without prior verification. In addition to providing ongoing supervision, it is important to conduct regular audits and to analyse the effectiveness of the supervisory measures that have been implemented. Another important aspect is to enable people about whom decisions are made by AI to obtain information about the system's operation and the legal measures available if they want to challenge the outcome of a decision.

As can be seen, extensive obligations are held by the deployers of high-risk AI systems, and these are only a few of them. Hence a temptation to classify a system as limited-risk instead of high-risk may be present. This issue will be discussed in detail later in this paper, as it is one of the main challenges for Member States in the area of market surveillance.

2. The administration of justice

Regarding the administration of justice, a high-risk AI system is one that is intended to be used by or on behalf of a judicial authority to assist it in researching and interpreting facts and the law and applying the law to a concrete set of facts, or used in a similar way in alternative dispute resolutions. This category refers to judicial authorities, which means courts. The The scope of application indicates that systems intended for use by judges and registrars, as well as by assistants and judicial trainees involved in adjudicatory support activities, are covered. The Court of Justice of the European Union has analysed the concept of a 'judicial authority' in the context of

whether a public prosecutor is a judicial authority entitled to issue a European Arrest Warrant. The organisation of the public prosecutor's office varies between Member States; in some, the prosecution service has strong links with the executive and may be subject to government instruction, while in others, it is independent, with prosecutors forming part of the judiciary. In these jurisdictions, prosecutors are considered to be organs of the judiciary (Judgment of the CJEU, 2019a; Judgment of the CJEU, 2019b; Perrodet, 2002).

Systems that replace judicial authorities in decision-making or other activities performed in the adjudication process, such as the assessment of legal definitions, the reconstruction of facts or the assessment of evidence, are prohibited. Nevertheless, systems can be used to support adjudicators in this respect. The Regulation identifies four areas of application, indicating that these kind of systems should be considered high-risk: research and interpretation of facts; research and interpretation of the law; application of the law to a specific factual situation; and use in a similar way in alternative dispute resolutions. However, the meaning of these terms is not entirely clear and needs to be discussed. AI systems that examine and interpret the facts in criminal, civil, administrative or other proceedings recognise certain patterns in a training dataset and predict whether a given set of facts indicates, for example, that a criminal offence has been committed, a contract has been performed improperly or an erroneous administrative decision has been issued.

Systems used for the examination and interpretation of legal provisions provide links between provisions or legal acts and present relevant case law, interpretations or lines of jurisprudence. They can also independently find the meaning of a provision based on learned interpretations of the same concepts in other provisions of the same or other legal acts, and in available legal definitions (Binkowski, 2023). In general, the vast majority of AI used in the legal industry is operated by law firms, their clients and, albeit less frequently, law-enforcement agencies. These tools are sometimes intended for use by courts; an example is a tool that was developed in France for anonymising court decisions (Vucheva et al., 2020, p. 189). However, as indicated above, this tool would not be considered a high-risk system under the AI Act. Applying the law to a specific factual situation involves subsumption (Cyras & Lachmayer, 2023, pp. 187–190; Zienowicz, 2019). Thus high-risk AI systems will be those that determine, on the basis of factual input, a proposed legal definition, a prohibited contractual provision or a liability regime, for example.

AI systems used in a similar manner in alternative dispute resolution are also high-risk. The Polish Ultima Ratio platform, for example, is an electronic arbitration court operated by the Electronic Arbitration and Mediation Centre at the Association of Notaries of the Republic of Poland in Warsaw that deals with the recognition of commercial disputes in domestic and international trade. Currently, work is underway to introduce an AI system to support the arbitrators. This system will automatically prepare a draft award, with its reasons. To this end, the system will process

into data the statements of the parties which are collected during the proceedings. Using mechanisms for grouping similar cases, it will be able to predict the most likely outcome of a given case. It is also intended that the system will support the arbitrator throughout the proceedings by providing information on the course and outcome of similar cases and presenting excerpts from the reasoning in other awards (Ultima Ratio, n.d.). However, there are disputes over whether arbitration courts are part of the administration of justice (Bookman, 2021). The EU concept of judicial authority suggests that it is most likely that this issue is decided on a case-by-case basis, depending on the design of the national legislation, the status of the authority and the EU instrument to be assessed.

It should be noted that although the judicial area is recognised as being particularly vulnerable to the infringement of individuals' fundamental rights, the AI Act identifies only a few categories of tools that should be considered high-risk within this space. These are systems that have an impact, or are likely to have an impact, on the decision-making processes in a case before a court. This interpretation is also indicated by the wording of Article 6(3) of the AI Act. These systems pose a far greater threat to the rule of law (Kouroutakis, 2024) and the right to a fair trial than others, because impartiality and independence in the judiciary are fundamental to both of these values (see Article 6(1) of the European Convention on Human Rights and Article 47 of the Charter of Fundamental Rights of the European Union). Where judicial decisions are influenced by analyses produced by AI systems, the independence of the judiciary may be undermined. Such analyses can reflect design choices made by the private companies that develop these systems, as well as variables that, under the rule of law, should not influence judicial decision-making. As a result, external interests, including those of private technology providers involved in the design of the systems, may indirectly affect judicial outcomes, thereby calling into question the independence of the judges. Many systems based on AI technology fall outside the above category, despite their use by the judiciary being advocated by doctrine, practitioners and policymakers (Abiodun & Lekan, 2020; Aini, 2020; Donohue, 2019; Lupo, 2019; Perry, 2017, p. 29). These include, for example, systems for the transcription of hearings or machine translation, which should be considered as general-purpose AI (Kiejnich-Kruk, 2024, 2025).

Bearing in mind the considerations presented so far, the recommendations addressed to policymakers focus on three key areas: a framework for the oversight and verification of the risk classification of AI systems by deployers; appropriate training for deployers; and a 'building blocks' strategy in the digitalisation of the judiciary. First, the research indicates that human rights risk assessments are often conducted in an informal manner, and deployers may be unaware of the specific risks posed by a given AI system. Consequently, such systems may be misclassified: the most significant risk arises when a system is incorrectly classified as limited-risk rather than high-risk. In the judicial context, this danger is particularly acute. This stems from

Article 6(3) of the AI Act, which requires an assessment of whether a system poses a significant risk to the fundamental rights of individuals, including cases where the system is deemed not to meaningfully impact the outcome of the decision-making process. As decision-making lies at the core of the administration of justice, such assessments require particular caution and careful consideration; therefore an effective system of verification and oversight must be established to ensure that AI systems used within the judiciary are correctly classified. The AI Act provides supervisory (and supportive) mechanisms at multiple levels, and notably establishes oversight by both EU and national authorities, as well as reference tools prepared by the European Commission, such as the database provided for in Article 71 and the guidelines under Article 6(5). However, at the national level, defining the powers of market surveillance authorities precisely is particularly important. Whether these authorities exercise genuine, substantive control over the classification of systems as high-risk or merely conduct formal, superficial reviews depends on the national legislature.

The second area is closely linked to the first. There is a pressing need for accessible training and practical guidelines for deployers, who, unlike providers, may have limited knowledge of AI systems and their potential impact on various rights and interests; research in this field confirms this. Therefore properly structured training is necessary to raise awareness among deployers of potential human rights risks and to ensure that risk assessments are carried out appropriately to correctly classify systems. This training should also cover other obligations set out in the AI Act, such as conducting FRIAs, event documentation, serious incident reporting and properly implementing human oversight requirements.

Third, initiatives that introduce artificial intelligence into the judiciary are desirable and worthy of support, whether to assist with decision-making or to streamline administrative tasks. However, in countries where the digitalisation of the judiciary is still in its infancy, financial and human resources should initially be allocated to the foundational phases of computerisation. This includes digitalising case files, implementing systems for electronic signatures, developing tools for anonymising judgments and calculating procedural deadlines, integrating public administration systems, establishing secure electronic communication channels, transcribing hearings and trials, and providing support for machine translation (Vucheva et al., 2020, Annex II). Although these systems use AI technologies, they are not primarily designed to support judicial decision-making and therefore do not fall within the high-risk categories discussed above. Consequently, they are not subject to the stringent requirements applicable to high-risk AI systems under the AI Act. Implementing such systems will enable the effective implementation of further projects. It is not possible to skip any of the stages of computerising justice, either technologically or socially, so it is therefore necessary to build the foundations and components of the systems according to the schedule that is adopted. This avoids duplication of errors, which can occur if a technological solution implemented in multiple products is not simultaneously verified. It also enables the system

to address the challenges associated with the implementation of high-risk AI systems, including cybersecurity, data protection, reporting, human oversight and risk minimisation (Kiejnich-Kruk, 2025).

3. Democratic processes

The second category relates to AI systems designed to influence election or referendum outcomes or the voting behaviour of individuals but does not include AI systems with results that individuals are not directly exposed to, such as tools used to organise, optimise or structure political campaigns from an administrative or logistical point of view. Some possible examples of AI-based tools in electoral processes could be AI systems used to deliver political advertising or profile voters, including microtargeting and amplification techniques, to process or count ballots or maintain voting lists, to identify cybersecurity attacks, to perform voter data analysis and predictive analytics, to counter biased content, to moderate electoral content and to provide assistance to voters with chatbot-based systems.

According to a UNESCO guide (Krimmer et al., 2022, p. 20), AI has the potential to enhance electoral processes. AI-based tools can reach a significant number of voters and engage them through personalised communication tailored to their individual preferences and behaviours. AI-based chatbots can provide real-time information about voting locations, candidates' manifestos and voting procedures, thereby making the electoral process more accessible and transparent. However, technological developments are also creating previously unknown threats to democracy and electoral processes. Concerns relating to future elections, including those anticipated for 2028 (USA), are already being discussed in the public sphere (Booth, 2026) and primarily concentrate on two areas: deepfakes and microtargeting. These practices will first be examined in detail, followed by an analysis of their implications for fundamental rights. Building on this assessment, a set of policy recommendations will be formulated.

On a large scale, the generation of false content – deepfakes – in political advertisements has become a means of misleading the public about candidates' claims and positions and about whether certain events actually took place. Under the AI Act, such content must clearly identify the source as AI and disclose that it is artificially generated (see Article 50(4)). For example, during the last US presidential campaign a fake video was created showing President Biden urging his supporters not to vote in the primaries; a political opponent of the incumbent president admitted to creating and distributing the footage (Michałkiewicz-Kądziela, 2024). However, according to Election-Watch.EU, the use of AI-generated content in online campaigning has been detected in only seven EU Member States: Germany, Denmark, Spain, Croatia, Ireland, Portugal and Sweden. In Germany, the most prominent case involved a deep-

fake video created by left-wing activists which depicted Chancellor Scholz calling for a ban on Alternative für Deutschland (AfD). Overall, however, politicians and groups associated with the AfD appear to be the most frequent users of deepfake content for their own purposes; one example is the mass circulation of deepfake audio recordings aimed at discrediting political opponents (European Partnership for Democracy, 2024, p. 12).

AI technology enables the analysis of voter data, including demographics, social media activity and previous voting behaviour. Political campaigns use AI to create detailed voter profiles, enabling politicians to tailor their messages to specific groups, for example, targeting radical content at one group and moderate content at another. This targeted approach can significantly increase the effectiveness of a campaign strategy. AI-based sentiment analysis tools can scan social media platforms, news articles and other content to gauge public opinion on various issues and candidates. With this data, campaigns can adjust their strategies in real time without having to wait for poll results, which are often published late and are based on the views of a relatively small group of people. Predictive AI enables campaigns to use available data to microtarget voters with personalised advertising and fundraising requests (Krimmer et al., 2022, p. 92). On the one hand, such tools can level the playing field for smaller campaigns, increasing their reach and enabling them to engage new audiences. On the other, they can manipulate voters' emotions.

For example, allegations of voter manipulation have been raised in relation to the UK's EU referendum, also known as the Brexit referendum. An investigation into the referendum by the UK Information Commissioner's Office found that pro-Brexit campaign groups had misused Facebook users' personal data for political marketing purposes, targeting political content at people who did not wish to receive it (Day, 2020; Risso, 2018). Another example relates to the annulment of the 2024 presidential election in Romania; the Romanian Constitutional Court cited several reasons for its annulment decision, including third-party campaign financing and access to undisclosed and unregulated funds for digital campaigning. Other reasons were the use of non-transparent digital technologies and artificial intelligence in campaigning, which violates electoral law, and the increased online exposure of candidates, which exerts undue influence on voters beyond public control. The Court also cited weak oversight by election management bodies, which lacked the resources to effectively supervise online advertising spending carried out through digital networks and platforms (International Foundation for Electoral Systems, 2024).

The AI systems mentioned above are focused on the so-called microtargeting of specific messages, the analysis of social emotions and the analysis of a person's world view in order to direct the appropriate message to them (in terms of both content and form), but there are also systems that allow for the artificial generation of online traffic. Expressions of approval for particular content on social media accounts that do not belong to real people certainly influence the behaviour of voters and conse-

quently the outcomes of elections themselves. The real challenge for public actors in this field is to control and verify whether high-risk systems have actually been used. A lack of transparency by election staff in this regard may raise justified doubts.

Given these risks, AI systems that generate artificial materials for electoral campaigns, distribute these materials and select the voters to whom the materials will be presented are considered high-risk. These systems pose a particular threat to democracy and individual freedoms, such as freedom of speech and the freedom to vote in accordance with one's beliefs without external influence. As the Preamble to the AI Act refers to individual rights, it also involves the right to vote and the right to be elected (these systems can influence how and for whom a person votes). AI-driven profiling, targeted disinformation and deepfake content can influence public perception of candidates unfairly and distort competition. Such practices risk undermining the principle of equal opportunity in electoral participation and may compromise the integrity of the democratic process. In order to safeguard this fundamental right, legal and regulatory frameworks must ensure transparency in the use of AI in campaigning, prevent discriminatory or manipulative practices and provide effective remedies for candidates whose electoral rights have been infringed by AI-enabled interventions.

AI-driven microtargeting, particularly when facilitated by generative AI, raises substantial concerns relating to data protection, manipulation and accuracy. Both the selection of target groups and the platforms used to deliver political advertising risk creating or exacerbating inequities, as electoral management bodies (EMBs) may disproportionately reach certain subgroups of the electorate (Ali et al., 2019). Data protection and data minimisation have therefore become priority concerns. Electoral datasets must be representative, secure and restricted to what is necessary to ensure inclusivity without compromising individual rights. The General Data Protection Regulation's (GDPR) principle of data minimisation requires that only data which is necessary for a defined purpose be processed. Applying this principle in the context of AI development, particularly during the training phase, poses significant challenges given the data-intensive nature of effective algorithmic training: large datasets are often relied upon to reduce bias and enhance model performance, which may initially appear to be at odds with the requirement of data minimisation. However, the GDPR allows for a degree of flexibility in the interpretation of 'necessity', acknowledging that extensive data collection may be justified at early stages, provided that data volumes are subsequently reduced. Accordingly, AI developers are required to implement robust filtering and deletion mechanisms to ensure that unnecessary data is removed once the training process is complete (Renaissance Numérique, 2025).

The use of AI systems also heightens the risk of foreign interference in electoral processes: advanced AI tools can enable external actors to produce and disseminate highly targeted disinformation at scale, manipulate online discourse and impersonate domestic political figures or institutions with increased credibility. Through techniques such as deepfakes, automated social media accounts and AI-driven mi-

crotargeting, foreign actors may seek to influence voter perceptions, suppress turnout or undermine trust in democratic institutions. Such practices may undermine the integrity of elections, violate principles of sovereignty and infringe upon voters' rights to free and informed participation (Farantouris & Pipis, 2025, p. 12).

There are other threats to human rights. AI-based verification methods may wrongfully disenfranchise legitimate voters, and increasing policing at polling sites may suppress voter turnout rates, impact electoral outcomes and reduce trust in the process (Padmanabhan et al., 2023). Empirical evidence highlights these risks: the accuracy of signature-based or biometric matching systems may be quite low, creating a significant risk of disenfranchising eligible voters (Hussain et al., 2015). In addition, the deployment of large language model (LLM) chatbots in electoral management presents serious concerns regarding the reliability of information. EMBs must therefore undertake extensive testing and auditing to prevent hallucinations and the dissemination of false or misleading information (Rawte et al., 2023). Moreover, excessive reliance on AI systems for misinformation detection may cause EMBs to overlook emerging narratives or voter concerns, particularly on private messaging platforms where automated monitoring is limited (Juneja, 2024, pp. 12–30).

At the same time, AI-driven fact-checking tools can play a crucial role in countering false narratives. Ensuring that these tools are widely accessible and effectively integrated into electoral processes can help mitigate the risks posed by AI-enabled disinformation. Fairness and non-discrimination constitute key ethical considerations in this context. AI systems deployed in elections must be designed to avoid bias and to ensure that they do not disproportionately affect specific groups of voters; for example, AI-based predictive analytics or voter profiling may unintentionally reinforce existing societal biases. Consequently, regulatory oversight is necessary to mandate fairness audits, ensuring that AI systems treat all voter groups equitably and do not perpetuate discriminatory outcomes (Itumeleng & Esiefarienrhe, 2024, p. 3217). One should bear in mind that systems intended for administrative tasks, such as updating voter lists, verifying voters, reporting on resource allocation and campaign spending, and measuring voter turnout in real time, have been exempted from the Regulation.

Both detecting the use of a specific system and the procedure for associating that system with a given actor (the entity using the system) may prove to be very complex. At the same time, these steps are crucial for assessing whether the entity has fulfilled its obligations under the AI Act and, further, whether the system can be considered to have been used correctly from the point of view of the protection of fundamental rights. It seems that a national legislative policy should focus on the following elements:

Public authorities should establish a robust system of verification and oversight to ensure the correct classification of AI systems as prohibited, high-risk or limited-risk;

It is necessary to introduce legal requirements for transparent declarations (and limits) regarding the use of AI systems in the course of election campaigns and in

elections (or referendums) themselves, not only from the entities directly involved in their conduct (political parties or EMBs), but also from all related entities;

There needs to be collaboration with internet service providers, including traditional media and social media, in the control of content related to elections and referendums, the broadcasters of such content and related entities (accounts), and methods of use.

The most important questions are how to classify a given system as prohibited, high-risk or limited-risk, and how to identify appropriate responsibilities and risk-mitigation tools. As noted above, such assessments are often conducted in a relatively informal manner. Relevant actors may be inclined to assign systems to a lower-risk category, partly because this entails fewer regulatory obligations but also due to limited awareness of human rights-related risks. For this reason, public bodies have a crucial role to play in establishing effective control and verification mechanisms to ensure that AI systems are properly classified and that deployers comply with the obligations imposed by the AI Act. This area of concern closely resembles the one discussed above in relation to judicial processes.

In the second area, numerous stakeholders have called for a coherent legal and ethical framework (Juneja, 2024; Nikolich, 2025; TIAL, 2025). EMBs should assess AI use cases against existing administrative practices, focusing on areas where AI may enhance current processes, and should undertake comprehensive evaluations of both the costs and benefits of implementation. Where feasible, EMBs and political actors should ensure meaningful human oversight of AI systems and treat AI as complementary to existing strategies rather than as a substitute for them. At the same time, all actors involved should adopt high standards of transparency, interpretability and accountability, both for AI systems developed internally and for those supplied by external vendors. Any AI-generated content should be clearly labelled.

A further pressing concern relates to misinformation and disinformation campaigns targeting electoral administration. Such campaigns may aim to confuse voters regarding the timing, location or procedural requirements of elections, thereby undermining public confidence in the integrity and legitimacy of the electoral process. The use of AI to generate and disseminate disinformation, including through deepfake videos and automated bot networks, presents a serious ethical and regulatory challenge. AI technologies enable the rapid and large-scale spread of false or misleading information, potentially influencing voter behaviour and compromising democratic integrity. Regulatory frameworks should therefore include specific provisions to limit the use of AI in the creation and dissemination of disinformation.

In the third area, EMBs should conduct thorough and continuous audits of AI systems, covering security, performance and ethical compliance. National legislation should complement EU-level instruments, in particular the Digital Services Act (DSA). The DSA provides, inter alia, for retention orders and for the investigation of potential infringements of Articles 34(1), 34(2) and 35(1), which concern obligations

to mitigate systemic risks, including those linked to fraudulent use and coordinated inauthentic behaviour. Such tools were employed in the European Commission's investigation concerning the legality of the presidential elections in Romania in 2024.

Moreover, the European Commission has issued guidelines addressed to providers of very large online platforms and very large online search engines concerning the mitigation of systemic risks in electoral processes (European Commission, 2024). These guidelines should be taken into account when assessing platform conduct. It is therefore essential that such platforms cooperate with public authorities, in compliance with the law, in order to limit harmful practices affecting electoral processes.

It should also be noted that the interplay between the AI Act and the DSA has been widely analysed in academic literature. Very large online platforms and search engines may be subject to systemic risk-assessment duties under both the AI Act and the DSA simultaneously, particularly where general-purpose AI models are integrated into intermediary services. More broadly, concerns have been expressed that the cumulative effect of the EU's digital regulatory framework – including, for example, the GDPR, with its requirement to conduct Data Protection Impact Assessments (Hohmann & Kollár, 2025; Levitina, 2025; Sarra, 2025; Sartor & Lagioia, 2020; Ufert, 2020), alongside the FRIAs required under the AI Act – may disproportionately burden European AI innovators (Graux et al., 2025). Intermediary service providers, such as online platforms and search engines, that develop, deploy or integrate AI systems (for example in recommender systems or content-moderation tools) may face cumulative transparency and risk-assessment obligations. While these obligations are not contradictory, their combined effect may increase the regulatory burden. Nevertheless, from the perspective of human rights protection, overlapping obligations do not in themselves constitute a threat. The DSA's content-moderation framework and the AI Act's requirements for high-risk AI systems may intersect, particularly in relation to AI-driven moderation tools. Both the DSA and the AI Act require platforms to assess and mitigate systemic risks, including those arising from the use of AI systems.

EMBs should also bear in mind that private messaging and email services largely fall outside the DSA's hosting service regime. Consequently, AI-powered chatbots operating within such environments are not clearly subject to the same regulatory obligations as online platforms. This creates a regulatory gap and presents a challenge for public authorities, as providers of these services are not bound by obligations equivalent to those imposed on platforms with regard to the spread of misinformation and disinformation.

Conclusion

The EU legislature has classified certain AI systems deployed in the administration of justice and in democratic processes as high-risk. These areas were considered together during the legislative process, as they pose risks to similar values, interests and, above all, fundamental rights. The fundamental rights at risk in the deployment of AI systems across both judicial and electoral processes are the right to a fair trial, the right to an effective remedy, the presumption of innocence, equality of arms and the right to defence, as well as freedom of expression, the freedom to vote according to one's convictions without undue influence and the right to be elected.

A core challenge for justice systems lies in distinguishing, within the broader digitalisation of judicial procedures, which systems qualify as high-risk AI and which fall outside that category. The use of high-risk systems entails a range of obligations aimed at mitigating risks to fundamental rights. Accordingly, policymakers should prioritise the development of a robust oversight and verification framework to ensure accurate system classification, coupled with targeted training for deployers to support compliance with these obligations. Strengthening these mechanisms would significantly enhance the protection afforded to individuals whose cases may be influenced by the use of such technologies.

In the electoral sphere, the enforcement of ethical and legal safeguards governing the use of AI presents equally complex challenges. Given that many election-related risks stem from the dissemination of information – whether accurate or misleading – concerning candidates, voting procedures or the electoral process more broadly, and considering that online platforms constitute the primary venues for such content, effective cooperation with these platforms is essential. Although the obligations arising under the DSA, the AI Act and related digital regulations may impose considerable burdens on intermediaries, they remain justified from the standpoint of safeguarding human rights. A sensible policy direction would therefore involve establishing legal requirements for transparent declarations and clear limitations concerning the use of AI systems during electoral campaigns, together with structured collaboration with internet platforms in monitoring election-related content, identifying entities responsible for its dissemination and scrutinising the methods through which AI tools are employed.

This article does not seek to exhaust the complexity of the issues examined, nor do the challenges and recommendations presented constitute a comprehensive list. They are intentionally general in scope: the objective has not been to propose fully formed legislative solutions but rather to outline key directions for further reflection. The findings underscore the need for continued scholarly inquiry in this field, while the recommendations provided serve as a valuable point of departure for academic debate as well as for policymakers engaged in shaping the future regulatory landscape.

REFERENCES

Abiodun, O., & Lekan, A. (2020). Exploring the potentials of artificial intelligence in the judiciary. *International Journal of Engineering Applied Sciences and Technology*, *5*(8), 23–27.

Aini, G. (2020). A summary of the research on the judicial application of artificial intelligence. *Chinese Studies*, *9*, 14–28.

Ali, M., Sapiezynski, P., Bogen, M., Korolova, A., Mislove, A., & Rieke, A. (2019). Discrimination through optimization: How Facebook's ad delivery can lead to skewed outcomes. *arXiv*. https://doi.org/10.48550/arXiv.1904.02095

Binkowski, K. (2023). Sztuczna inteligencja a wykładnia prawa – propozycja zastosowania systemów AI do ustalania założenia o racjonalnym prawodawcy. *ZeszytPrawniczy, U. A. M., 13*, 7–17.

Bookman, P. K. (2021). Arbitral courts. *Virginia Journal of International Law*, *61*, 179–184, 201–213.

Booth, R. (2026, 22 January). Experts warn of threat to democracy from 'AI bot swarms' infesting social media. *The Guardian*. https://www.theguardian.com/technology/2026/jan/22/experts-warn-of-threat-to-democracy-by-ai-bot-swarms-infesting-social-media

Brożek, B., Furman, M., Jakubiec, M., & Kucharzyk, B. (2024). The black box problem revisited: Real and imaginary challenges for automated legal decision making. *Artificial Intelligence and Law*, *32*, 427–440.

Cyras, V., & Lachmayer, F. (2023). *Essays on the visualisation of legal informatics*. Springer International Publishing.

Day, P. (2020). Cambridge Analytica and voter privacy. *Georgetown Law Technology Review*, *4*(2), 583–608.

Donohue, M. (2019). A replacement for Justitia's scales? Machine learning's role in sentencing. *Harvard Journal of Law and Technology*, *32*(2), 657–678.

European Commission. (2022). Commission Guidelines for Providers of Very Large Online Platforms and Very Large Online Search Engines on the Mitigation of Systemic Risks for Electoral Processes Pursuant to Article 35(3) of Regulation (EU) 2022/2065 (Text with EEA Relevance) (C/2024/3014).

European Commission. (2024, 26 April). Communication from the Commission – Commission Guidelines for Providers of Very Large Online Platforms and Very Large Online Search Engines on the Mitigation of Systemic Risks for Electoral Processes Pursuant to Article 35(3) of Regulation (EU) 2022/2065, C/2024/2537 (O. J. C C/2024/3014, 26.04.2024).

European Commission. (2024a). *Commission, online platforms and civil society increase monitoring during Romanian elections*. https://ec.europa.eu/commission/presscorner/detail/en/ip_24_6243

European Commission. (2024b). *Commission opens formal proceedings against TikTok on election risks under the Digital Services Act*. https://ec.europa.eu/commission/presscorner/detail/en/ip_24_6487

European Parliament and the Council. (2022, 19 October). Regulation on a Single Market for Digital Services and Amending Directive 2000/31/EC (Digital Services Act) (Text with EEA relevance) (2022/2065) (O. J. L 277, 27.10.2022, pp. 1–102).

European Parliament and the Council. (2024, 12 July). Regulation Laying Down Harmonised Rules on Artificial Intelligence and Amending Regulations (EC) No. 300/2008 (EU) No. 167/2013 (EU)

No. 168/2013 (EU) 2018/858 (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act) (Text with EEA Relevance) (2024/1689) (O. J. L, 2024/1689, 12.07.2024).

European Partnership for Democracy. (2024). *The EU's Artificial Intelligence Act and its impact on electoral processes: A human rights-based approach*. https://epd.eu/content/uploads/2024/09/AI-and-elections.pdf

Farantouris, N., & Pipis, T. (2025, October). *AI in the democratic sphere and the electoral process*. https://farantouris.eu/wp-content/uploads/2025/10/Research-Paper-AI-Disinformation-.pdf

FRA (2020). *Getting the future right: Artificial intelligence and fundamental rights*. Publications Office of the European Union.

FRA (2025). *Assessing high-risk AI: Fundamental rights risks*. https://fra.europa.eu/sites/default/files/fra_uploads/fra-2025-assessing-high-risk-ai-fundamental-rights-risks_en.pdf

Fülöp, T., & Poindl, P. (2025). Article 27. In C. N. Pehlivan, N. Forgó, & P. Valcke (Eds.), *The EU Artificial Intelligence (AI) Act: A commentary* (pp. 553–573). Wolters Kluwer.

Graux, H., Garstka, K., Murali, N., Cave, J., & Botterman, M. (2025). *Interplay between the AI Act and the EU digital legislative framework*. European Parliament. https://www.europarl.europa.eu/RegData/etudes/ATAG/2025/778577/ECTI_ATA(2025)778577_EN.pdf

Hassija, V., Chamola, V., Mahapatra, A., Singal, A., Goel, D., Huang, K., Scardapane, S., Spinelli, I., Mahmud, M., & Hussain, A. (2024). Interpreting black-box models: A review on explainable artificial intelligence. *Cognitive Computation*, *16*, 45–74.

Hohmann, B., & Kollár, G. (2025). Reflections on the data protection compliance of AI systems under the EU AI Act. *Cogent Social Sciences*, *11*(1). https://doi.org/10.1080/23311886.2025.2560654

Hussain, R., Raza, A., Siddiqi, I., Khurshid, K., & Djeddi, C. (2015). A comprehensive survey of handwritten document benchmarks: Structure, usage and evaluation. *EURASIP Journal on Image and Video Processing*, *2015*(1), Article 46. https://doi.org/10.1186/s13640–015-0102–5

International Foundation for Electoral Systems. (2024). *The Romanian 2024 election annulment: Addressing emerging threats to electoral integrity*. https://www.ifes.org/publications/romanian-2024-election-annulment-addressing-emerging-threats-electoral-integrity

Itumeleng, M. M., & Esiefarienrhe, B. M. (2024). The impact of artificial intelligence, ethical implications and technologies on the electoral process. *E-Journal of Humanities, Arts and Social Sciences*, *5*(16), 3211–3219. https://doi.org/10.38159/ehass.202451641

Judgment of the CJEU of 27 May 2019 on the case of *Minister for Justice and Equality v. OG and PI*, C 508/18.

Judgment of the CJEU of 27 May 2019 on the case of *PF*, C-509/18.

Juneja, P. (2024). *Artificial intelligence for electoral management*. International Institute for Democracy and Electoral Assistance. https://doi.org/10.31752/idea.2024.31

Kiejnich-Kruk, K. (2024). Lost in translation: Implementation of the right to a translator through the use of machine translators in the light of EU and Polish Law. *Ruch Prawniczy, Ekonomiczny i Społeczny*, *84*(1), 61–81.

Kiejnich-Kruk, K. (2025). Building blocks – strategia cyfryzacji wymiaru sprawiedliwości. Perspektywa estońska. *Przegląd Sądowy*, *3*, 86–100.

Kouroutakis, A. (2024). Rule of law in the AI era: Addressing accountability, and the digital divide. *Discover Artificial Intelligence*, *4*, 115. https://doi.org/10.1007/s44163–024-00191–8

Krimmer, R., Rabitsch, A., Kužel, R., Achler, M., & Licht, N. (2022). *Elections in digital times: A guide for electoral practitioners*. The United Nations Educational, Scientific and Cultural Organization.

Levitina, A. (2025). Humans in automated decision-making under the GDPR and AI Act. *Revista CIDOB d'Afers Internacionals, 138*, 121–144.

Lupo, G. (2019). Regulating (artificial) intelligence in justice: How normative frameworks protect citizens from the risks related to AI use in the judiciary. *European Quarterly of Political Attitudes and Mentalities*, *8*(2), 75–96.

Mentelero, A. (2024). The Fundamental Rights Impact Assessment (FRIA) in the AI Act: Roots, legal obligations and key elements for a model template. *Computer Law & Security Review*, *54, article number: 106020*.

Michałkiewicz-Kądziela, E. (2024). The impact of deepfakes on elections and methods of combating disinformation in the virtual world. *Teka Komisji Prawniczej PAN Oddział w Lublinie*, *17*(1), 152–153.

Nikolich, A. (2025). A unified code of ethics and conduct for AI and trustworthy elections. In: B. Srivastava, A. Nikolich, A. Hickerson, & T. Koppel (Eds.), *Promise: Promoting AI's safe usage for elections* (pp. 279–290). Springer. https://link.springer.com/chapter/10.1007/978–3-031–89853-2_17

Padmanabhan, D., Simoes, S., & MacCarthaigh, M. (2023). AI and core electoral processes: Mapping the horizons. *AI Magazine*, *44*(3), 218–239. https://doi.org/10.1002/aaai.12105

Perrodet, A. (2002). The public prosecutor. In M. Delmas-Marty & J. R. Spencer (Eds.), *European Criminal Procedure* (pp. 415–455). Cambridge University Press.

Perry, M. (2017). iDecide: Administrative decision-making in the digital world. *Australian Law Journal*, *91*, 29–41.

Pinto, R., Mettler, T., & Taisch, M. (2013). Managing supplier delivery reliability risk under limited information: Foundations for a human-in-the-loop DSS. *Decision Support System*, *54*(2), 1076–1084.

Rawte, V., Sheth, A., & Das, A. (2023). A survey of hallucination in large foundation models. *arXiv*. https://doi.org/10.48550/arXiv.2309.05922

Renaissance Numérique. (2025). *Interactions and overlaps between the GDPR and AI Act, with Etienne Drouard*. https://www.renaissancenumerique.org/en/publications/interactions-and-overlaps-between-the-gdpr-and-ai-act-with-etienne-drouard/

Risso, L. (2018). Harvesting your soul? Cambridge Analytica and Brexit. In C. Jansohn (Ed.), *Brexit means Brexit?* (pp. 75–85). Akademie der Wissenschaften und der Literatur.

Sarra, C. (2025). Artificial intelligence in decision-making: A test of consistency between the EU AI Act and the GDPR. *Athens Journal of Law, 11*(1), 45–62.

Sartor, G., & Lagioia, F. (2020). The impact of the General Data Protection Regulation (GDPR) on artificial intelligence. *Publications Office of the European Union*.

TIAL (2025). *White paper #001: Safeguarding elections in the age of AI and synthetic content*. https://tial.org/publications/white-paper-001-safeguarding-elections-in-the-age-of-ai-and-synthetic-content/

Ufert, F. (2020). AI regulation through the lens of fundamental rights: How well does the GDPR address the challenges posed by AI? *European Papers*, 5(2), 1087–1097.

Ultima Ratio (n.d.). *Sztuczna inteligencja w Ultima Ratio. Czy roboty zastąpią arbitrów?* Retrieved 5 February 2025, from https://ultimaratio.pl/blog/sztuczna-inteligencja-w-ultima-ratio-czy-roboty-zastapia-arbitrow

Vucheva, M., Rocha, M., Renard, R., & Stasinopolous, D. (2020). *Study on the use of innovative technologies in the justice field – Final report*. https://op.europa.eu/en/publication-detail/-/publication/4fb8e194-f634–11ea-991b-01aa75ed71a1/language-en

Weitkunat, R., & Bestle, M. (1990). Computerized Mackworth vigilance clock test. *Computer Methods and Programs in Biomedicine*, *32*(2), 147–149.

Zienowicz, T. A. (2019). Artificial intelligence i singularity w procesie stosowania prawa, *Prawo Mediów Elektronicznych*, *2*, 31–33.

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

sciendo

DOI: 10.15290/bsp.2026.31.01.08

Received: 07.08.2025
Accepted: 13.12.2025

Zeynep Ayata
Istanbul Policy Center, Sabancı University, Turkey
zeynep.ayata@sabanciuniv.edu

Gender Bias in AI Systems: A Critical Analysis of Regulatory Frameworks and Policy Responses

Abstract: The rapid proliferation of artificial intelligence systems has exposed pervasive gender biases that reflect and amplify existing societal inequalities, posing significant threats to gender equality and women's fundamental rights. This article examines gender bias in AI systems through both theoretical and regulatory lenses, analysing how these biases manifest and can be addressed through comprehensive policy frameworks. The first section provides a systematic literature review exploring how bias becomes embedded in algorithmic systems through biased training data, algorithmic design choices, and broader cultural contexts. The second section examines policy responses, comparing UNESCO's comprehensive recommendations with the European Union's Artificial Intelligence Act and referencing the Council of Europe Framework Convention on Artificial Intelligence. This analysis reveals a significant disconnect between aspirational frameworks and practical implementation, demonstrating that existing regulatory approaches inadequately address gender bias in AI and highlighting the urgent need for comprehensive integration of gender equality considerations into AI governance frameworks.

Keywords: gender bias, artificial intelligence, gender equality, EU AI Act, AI governance

Introduction

The rapid proliferation of artificial intelligence systems across virtually every sector of society has brought unprecedented opportunities for innovation and efficiency, yet it has simultaneously exposed deep-rooted biases that reflect and amplify existing societal inequalities. Among the most pervasive and concerning of these biases is gender discrimination, which manifests across AI applications, from facial recognition systems that misidentify women at alarming rates to hiring algorithms that systematically favour male candidates. As AI systems increasingly influence crit-

ical decisions affecting employment, healthcare, criminal justice, and access to services, the embedded gender biases within these technologies pose significant threats to gender equality and women's fundamental rights.

These biases emerge not in a vacuum, but against a backdrop of profound gender disparities in the technology sector itself. Women remain dramatically underrepresented in artificial intelligence development and research, constituting only 12% of AI researchers globally and a mere 6% of software developers (Manasi et al., 2022). This underrepresentation extends throughout the technology pipeline: women earn only 18% of computer science bachelor's degrees in the United States, hold 26% of computing-related jobs, and occupy just 25% of technical roles at major technology companies. In academic settings, women comprise only 22% of AI professors globally, declining to 16% at full professor level, while representing merely 18% of presenters at leading AI conferences. The gender gap widens further when we examine leadership positions, with women holding only 15% of AI research director positions at major technology companies and 10% of leadership roles in AI start-ups. These structural inequalities in who develops AI systems directly shape the technologies produced, as homogeneous development teams are less likely to identify potential biases or consider diverse user needs and experiences (O'Connor & Liu, 2024).

The intersection of gender and artificial intelligence represents a complex sociotechnical challenge that extends far beyond mere algorithmic fairness. Gender bias in AI systems emerges through multiple pathways: biased training data that reflects historical patterns of discrimination, algorithmic design choices made by predominantly male development teams, and the broader cultural contexts that shape how these technologies are conceived, developed, and deployed. From virtual assistants programmed with submissive feminine personas to medical AI systems trained primarily on male patients, these biases are not incidental flaws but structural features that require systematic analysis and intervention.

This article examines the multifaceted nature of gender bias in AI systems through both theoretical and regulatory lenses, analysing how these biases manifest, persist, and can be addressed through comprehensive policy frameworks. The first section provides a thorough review of existing literature on gender bias in AI, exploring theoretical frameworks that explain how bias becomes embedded in algorithmic systems and examining empirical studies that document the scope and impact of gender discrimination across various AI applications. This analysis reveals how AI systems often perpetuate existing inequalities while creating new forms of digital discrimination that disproportionately affect women and marginalized gender groups. The second section shifts focus to policy and regulatory responses, examining how international organizations like UNESCO and the United Nations are developing frameworks to address gender equality in AI governance. Particular attention is given to the European Union's Artificial Intelligence Act, the world's first comprehensive AI regulation, which offers both opportunities and limitations for addressing gen-

der bias in AI systems. The analysis also considers the Council of Europe Framework Convention on Artificial Intelligence, the first legally binding international treaty in this domain, which establishes equality and non-discrimination as fundamental principles. Through critical analysis of these regulatory frameworks, this article evaluates whether existing approaches adequately address the complex challenges of gender bias in AI or whether more targeted interventions are necessary to ensure that AI serves as a tool for advancing rather than undermining gender equality in the digital age.

1. Theoretical frameworks and comprehensive analyses of gender bias in AI systems

Scholars in technology studies, such as Orlikowski and Fountain, argue that technologies are not neutral but rather reflect the social contexts in which they are created and deployed (Fountain, 2004; Orlikowski, 1992). Gender bias, defined as prejudiced actions based on the perception that women are not equal to men in rights and dignity, becomes embedded in AI systems through biased training data, algorithmic design choices, and the broader cultural contexts that shape technology development. This bias manifests both through language patterns and visual representations, with AI systems often amplifying existing societal inequalities rather than simply reflecting them. The literature review in this section examines various quantitative and qualitative analyses conducted in this field, addressing both general theories on how AI generates gender biases and specific problems in areas such as facial recognition, labour markets, and healthcare services.

A comprehensive framework for analysing gender bias has been presented by O'Connor and Liu (2024), who examine how AI systems perpetuate existing biases. The authors developed a two-dimensional analytical framework that categorizes AI technologies based on their data sources (text versus images) and their relationship to gender bias (perpetuation versus mitigation). For text-based AI, they examined how Google Translate perpetuates gender stereotypes by consistently translating gender-neutral pronouns as male for professional occupations, particularly in STEM fields. This bias was so pronounced that while women make up 35.94% of occupations according to Bureau of Labor Statistics data, they were represented with female pronouns in only 11.76% of translations. Conversely, O'Connor and Liu highlight successful bias mitigation efforts by researchers who developed debiasing algorithms for word embeddings, reducing gender stereotypes in semantic associations from 19% to 6%. In the realm of image-based AI, O'Connor and Liu (2024) analyse Joy Buolamwini and Timnit Gebru's (2018) groundbreaking 'Gender shades' study, which revealed significant intersectional biases in commercial facial recognition systems. These systems showed error rates of 8.1% to 20.6% between male and female classifi-

cations, with darker-skinned females experiencing misclassification rates as high as 72.4%. The study's impact extended beyond academic circles, prompting direct responses from major technology companies like IBM and Microsoft, who acknowledged the bias and committed to improving their systems.

Manasi et al. (2022) focus particularly on virtual assistants and robotics through the lens of feminist theory and the concept of affective labour. Their study provides detailed analysis of virtual assistants like Siri, Alexa, and Cortana, and notes that these systems are deliberately designed with feminine characteristics, including voices, names, and submissive personalities, that reinforce traditional gender stereotypes. The authors point out that while Google Assistant avoids gendered naming, most virtual assistants come with feminine voices and are programmed to perform traditionally female-coded tasks such as scheduling, note-taking, and list-making. This 'anthropomorphization' process creates what the authors term a 'master–servant relationship' similar to domestic labour arrangements. Problematically, these systems often fail to recognize or appropriately respond to gendered experiences, such as when early versions of Siri could not comprehend statements about sexual violence. In examining robotics, the authors highlight how service robots in sectors like hospitality, healthcare, and retail – traditionally seen as 'women's terrain' – are increasingly feminized and designed to perform affective labour. Research shows that 'male' robots are deemed appropriate for security-related jobs while 'female' robots are selected for healthcare settings, reflecting broader societal gender biases. The authors note that AI systems promise 'the allure of objectivity without public accountability' while embedding social biases (Manasi et al. 2022, p. 301). This is exacerbated by the severe underrepresentation of women in AI development – only 12% of AI researchers are women, and they represent just 6% of software developers.

Otis et al. (2024) present comprehensive evidence of a significant and persistent gender gap in generative AI use worldwide. The researchers synthesized data from 18 studies encompassing over 143,000 individuals across diverse regions, sectors, and occupations, combined with internet traffic data from major AI platforms like ChatGPT, Claude, and Perplexity. Their findings reveal a remarkably consistent pattern: women are approximately 20% less likely than men to use generative AI tools, with this gap holding across nearly all the contexts examined. According to the authors, the scale and universality of this gender disparity is striking. Analysis of representative US samples shows gaps of 10–20 percentage points, with similar patterns observed among populations ranging from science postdocs to business owners to college students across multiple countries. Internet traffic data corroborates these survey findings, showing that women comprise only 42% of ChatGPT website users globally and just 27% of mobile app downloads. To test whether the gap stems from differential access to the technology, the researchers conducted a novel experiment in Kenya, offering 17,541 participants equal opportunity to try ChatGPT. Even with access equalized, women remained 13% less likely to adopt the technology, indicating

that simply providing access is insufficient to close the gender divide. This suggests deeper underlying mechanisms driving the disparity, including differences in knowledge and familiarity with AI tools, confidence in using the technology effectively, and perceptions about the ethics of AI usage.

An empirical study by Ahn et al. (2022) investigates how gender stereotypes influence consumer evaluations of AI agents' recommendations, and specifically examined the interaction between an AI's 'gender' and the type of product (utilitarian versus hedonic). The researchers explored whether people apply the same gender stereotypes to AI agents that they use in human interactions, and how this affects trust in AI recommendations for different product categories. The study carried out two experiments, involving 180 and 120 participants respectively, testing interactions with chatbots and AI speakers using recorded human voices. The findings revealed significant gender stereotype effects on perceptions of AI personalities. 'Female' AI agents were perceived as significantly warmer than 'male' AI agents, supporting traditional gender stereotypes, and 'male' AI agents were perceived as more competent than 'female' AI agents. More importantly, the study found crucial interaction effects that depended on the product type. For utilitarian products, participants showed more positive attitudes and higher purchase intentions when they were recommended by 'male' AI agents. Conversely, for hedonic products, participants responded more favourably to recommendations from 'female' AI agents.

Domnich and Anbarjafari (2021) investigated gender bias in deep-learning models for facial expression recognition, contributing to the broader field of Responsible AI by examining fairness in emotion recognition systems. The researchers conducted a comprehensive analysis using six different neural network architectures, systematically dividing both training and testing data by gender to create 'regular' models (trained on all data), 'male' models (trained only on male data), and 'female' models (trained only on female data). The key findings revealed significant variations in gender bias across different neural network architectures. The study found that models generally performed better on emotions that aligned with traditional gender stereotypes, with recognition of surprise being more accurate for 'males' and emotions like sadness and being upset better recognized in 'females'. Interestingly, happiness recognition remained relatively consistent across genders. The analysis revealed that more biased neural networks consistently showed larger accuracy gaps between 'male' and 'female' test sets.

Andrews and Bucher (2022) examine how AI systems used in hiring processes can perpetuate gender discrimination. Their paper analyses three main AI technologies used in hiring that potentially discriminate against women: CV scanning, one-way video interviews, and video game assessments. These seemingly neutral technologies can embed gender bias because they are often trained on data from predominantly male workforces, causing them to favour traditionally masculine traits and communication styles. Amazon's failed hiring algorithm serves as a promi-

nent example: after 500 attempts, the company's engineers could not create an unbiased system because their algorithm, trained on predominantly male employee data, systematically rejected women's CVs. It penalized applications containing the word 'women' and rejected candidates from women-only colleges, while sometimes recommending unqualified male candidates. The authors explain how these technologies perpetuate discrimination through various mechanisms. CV-scanning algorithms may favour 'active' verbs like 'executed' and 'captured' more commonly used by men, while penalizing collaborative language like 'we' that women often use. One-way video interviews can discriminate based on speech patterns, facial expressions, and communication styles that differ between genders due to socialization.

Lau (2023) examines the critical issue of gender bias in artificial intelligence systems used in women's healthcare, analysing the problem from legal, technological, and feminist perspectives across legal frameworks in the United Kingdom and Europe. The core argument centres on how androcentricity in medicine – the male body serving as the standard template – has created systemic biases that are now amplified through AI technologies. When AI systems are trained on historical medical data that predominantly reflects male experiences and biology, they perpetuate and amplify existing inequalities. For instance, women experience adverse drug reactions twice as often as men because clinical trials have historically excluded women, leading to dosing protocols based on male physiology. Similarly, conditions like acute myocardial infarction are often misdiagnosed in women because their symptoms differ from the male-centred diagnostic criteria that AI systems are trained to recognize.

As this literature review demonstrates, without deliberate action to close the gender gap in AI development and usage, generative AI risks not only perpetuating existing gender inequalities but potentially widening them, limiting society's ability to benefit from the diverse perspectives and contributions women could bring to this transformative technology. The evidence thus demonstrates that gender bias in AI systems is a multifaceted problem requiring comprehensive solutions across technical, social, and policy dimensions.

2. Policy and regulatory perspectives

In an interview with the UN organization UN Women (2025), Zinnya del Villar, a leading expert on responsible AI, explores how AI technologies, while transformative, can perpetuate and amplify existing gender inequalities when trained on biased data. Del Villar explains that AI gender bias occurs when systems learn from data filled with stereotypes, leading them to reflect and reinforce discriminatory patterns in their decision-making processes. The real-world impacts are significant and far-reaching: in healthcare, AI systems may focus more on male symptoms, potentially leading to misdiagnoses for women; voice assistants that default to female

voices reinforce stereotypes about women being suited for service roles; and language models often associate certain professions with specific genders. The report highlights documented cases, such as Amazon's discontinued AI recruitment tool from 2018 that favoured male CVs, and image recognition systems that have struggled to accurately identify women, particularly women of colour, with serious implications for law enforcement and public safety.

2.1. UNESCO recommendations: Integrating gender equality into AI principles

UNESCO's Global Dialogue on Gender Equality and AI (2020) identifies critical gaps in how gender considerations are addressed in AI ethics frameworks. The report emphasizes that gender equality must be treated as more than an add-on to existing principles, requiring instead a fundamental transformation in how AI systems are developed, deployed, and governed. The recommendations call for moving beyond technical fixes to address systemic inequalities embedded in AI development processes.

The integration of gender equality into AI principles must begin with inclusive development processes that ensure meaningful participation by gender equality experts and women throughout the principles' formulation, interpretation, application, monitoring, and recalibration. This participation should occur at all levels – intergovernmental, sectoral, and institutional – and must be sustained throughout the entire lifecycle of AI governance frameworks. Meaningful involvement by gender experts and women is essential because their lived experiences and specialized knowledge enable the identification of potential biases and discriminatory impacts that might otherwise remain invisible to homogeneous development teams. Gender experts bring critical analytical frameworks for understanding how power dynamics operate within technological systems, while women's participation ensures that diverse perspectives inform the interpretation and application of AI principles. This inclusive approach helps prevent the reproduction of existing inequalities and creates pathways for AI systems to actively advance gender equality. The process requires deliberate and thoughtful consideration of when gender should be made explicit versus implicit, with careful attention to where these references are placed within frameworks to ensure accountability and meaningful implementation rather than tokenistic inclusion.

Gender equality should be established as a stand-alone principle rather than being subsumed under broader categories like bias or fairness. UNESCO emphasizes that gender encompasses much larger concerns than algorithmic bias alone, including women's empowerment, representation in leadership roles, access to education and training opportunities, and participation in decision-making processes (UNESCO, 2020). The principle should be positioned prominently within frameworks, with clear implementation pathways and monitoring mechanisms. Effective integration requires adopting whole-society, systems-based, and lifecycle approaches that

consider AI's broader social and structural implications. This means addressing gender equality not just in specific algorithms or datasets, but throughout the entire AI ecosystem – from initial research and development through deployment, use, and ongoing monitoring. The approach must recognize relationships and power dynamics between different actors, on local to global scales, and address the responsibilities of both private and public sectors. Understanding these power dynamics is crucial because AI development and deployment occur within existing structures of gender inequality, where certain voices and interests dominate while others are marginalized. Power operates through multiple channels: in determining research priorities and funding allocations, in shaping technical standards and best practices, in controlling access to data and computational resources, and in defining what constitutes 'successful' AI implementation. Recognizing these dynamics helps identify whose interests are served by particular AI systems and whose are overlooked or harmed, enabling more equitable distribution of AI's benefits and more effective mitigation of its risks. This systemic view acknowledges that AI operates within existing social structures and can either reinforce or challenge gender inequalities.

The recommendations outline a three-dimensional approach to addressing gender equality in AI. First, avoiding harm requires the proactive identification and mitigation of AI's negative impacts on women and girls, including bias in algorithms, discriminatory outcomes, and reinforcement of harmful stereotypes. Second, increasing visibility involves ensuring that women's experiences, perspectives, and needs are represented in AI development and that gender implications are explicitly considered rather than overlooked. Third, contributing to empowerment means leveraging AI's potential to actively advance gender equality, challenge oppressive norms, and create opportunities for women's advancement in areas like education, economic participation, and political representation. This three-dimensional framework recognizes that gender equality in AI requires more than preventing discrimination – it demands proactive measures to empower women and transform existing power structures. By framing gender equality across these three dimensions, UNESCO emphasizes that AI governance must simultaneously protect against harms, ensure the representation and visibility of women's concerns, and actively promote women's empowerment and advancement. This comprehensive approach contrasts sharply with regulatory frameworks that focus primarily on harm prevention while neglecting the transformative potential of AI as a tool for advancing gender equality.

The UNESCO framework emphasizes the critical importance of intersectionality, recognizing that women's experiences vary significantly based on race, ethnicity, age, disability status, sexual orientation, geographic location, and socioeconomic status (UNESCO, 2020). AI principles must account for these multiple and overlapping forms of discrimination and ensure that solutions do not inadvertently harm marginalized groups while helping others. This requires diverse and inclusive teams in AI development that include not only women but also gender equality experts, repre-

sentatives from affected communities, and specialists in relevant domains where AI systems will be deployed.

Moving from principles to practice requires concrete mechanisms for implementation across multiple stakeholder groups. For the private sector, this includes establishing corporate governance mechanisms that integrate gender equality considerations, implementing bias detection and mitigation tools throughout the AI development lifecycle, creating diverse development teams with meaningful gender equality expertise, and conducting regular algorithmic impact assessments with gender-specific criteria. Government action should focus on developing appropriate policy frameworks, funding gender-responsive AI research and development, ensuring that procurement practices promote gender equality, and creating accountability mechanisms for AI systems used in public services.

The recommendations emphasize the need for robust monitoring and accountability mechanisms to ensure that gender equality commitments translate into measurable outcomes. This includes developing gender-responsive indicators for AI systems, establishing independent oversight bodies with gender equality expertise, creating transparent reporting requirements for AI developers and deployers, and implementing feedback mechanisms that centre the voices of affected women and marginalized communities. Regular assessment and recalibration of both principles and implementation strategies are essential to address emerging challenges and opportunities as AI technologies continue to evolve.

2.2. A general overview of the EU AI Act and the Council of Europe Framework Convention

The first-ever and most significant comprehensive regulation of AI is Regulation (EU) 2024/1689, known as the AI Act, adopted by the EU in 2024. The Act is therefore worth analysing from the point of view of gender policy and equality, as it might also constitute an inspiration or benchmark for regulation in other jurisdictions. Additionally, the Council of Europe Framework Convention on Artificial Intelligence, Human Rights, Democracy and the Rule of Law, adopted in May 2024 and opened for signature in September 2024, represents the first legally binding international treaty on AI. The Convention establishes human rights, democracy, and the rule of law as fundamental principles for AI systems, with equality and non-discrimination prominently featured among its core protections. The EU's participation in developing this Convention provides important context for understanding the Union's broader approach to AI regulation and gender equality. Although the AI Act will not be fully applicable until August 2026, it is important to examine the possible consequences of its implementation in terms of gender bias. This section will thus first account for the goals and general rules of the EU AI Act and will reference the Council of Europe Framework Convention, before examining in the subsequent section the specific treatment of gender equality within these frameworks.

The Artificial Intelligence Act, officially designated as Regulation (EU) 2024/1689 and enacted on 13 June 2024, represents the world's first comprehensive regulatory framework for artificial intelligence systems. It aims to improve the functioning of the internal market while promoting human-centric and trustworthy AI development, ensuring high levels of protection for health, safety, fundamental rights, democracy, the rule of law, and the environment against potential harmful effects of AI systems within the Union. The legislation adopts a risk-based approach to AI regulation, categorizing AI systems into different risk levels with corresponding obligations. At the most restrictive level, the Act prohibits certain AI practices deemed unacceptable, including AI systems that deploy subliminal techniques to materially distort human behaviour, exploit vulnerabilities of specific groups, implement social scoring systems leading to detrimental treatment, and create or expand facial recognition databases through untargeted scraping. The Act also heavily restricts real-time remote biometric identification systems in publicly accessible spaces for law enforcement purposes, permitting their use only in narrowly defined circumstances such as searching for victims of serious crimes or preventing terrorist attacks.

For high-risk AI systems, which include those used in critical infrastructure, education, employment, essential services, law enforcement, migration control, and democratic processes, the Act establishes mandatory requirements covering risk management, data governance, technical documentation, transparency, human oversight, and cybersecurity. These systems must undergo conformity assessments before market placement and bear a CE marking to indicate compliance. Providers must implement quality management systems, maintain detailed technical documentation, and establish post-market monitoring methods to track system performance throughout its lifecycle.

The Act introduces specific provisions for general-purpose AI models, particularly those with systemic risks identified by computational thresholds, such as models trained with more than 10^{25} floating point operations. Providers of these models must conduct model evaluations, assess and mitigate systemic risks, report serious incidents, and ensure adequate cybersecurity protection. The legislation encourages the development of codes of practice to demonstrate compliance and establishes the AI Office within the European Commission to monitor and enforce obligations for general-purpose AI models.

The governance structure includes the European Artificial Intelligence Board, composed of Member State representatives, a scientific panel of independent experts, and an advisory forum representing various stakeholders. Member States must designate national competent authorities for market surveillance and conformity assessment, with specific provisions for different sectors, including financial services and law enforcement. The Act provides for significant penalties, with administrative fines reaching up to EUR 35 million or 7% of worldwide annual turnover for prohibited AI

practices, and establishes procedures for market surveillance, incident reporting, and enforcement coordination across the Union.

The regulation will be implemented in phases, with prohibitions and general provisions applying from 2 February 2025, governance structures operational by 2 August 2025, obligations for general-purpose AI models effective from 2 August 2025, and the full regulation applying from 2 August 2026. This staggered implementation allows time for the development of the technical standards, codes of practice, and institutional frameworks necessary for effective enforcement, while providing legal certainty for AI developers and deployers across the European Union.

2.3. A critical assessment of the EU AI Act from a gender equality perspective

In order to analyse the Act from a gender equality perspective, we can start by examining its impact assessment report. It should first be noted that the report deals with and refers to gender equality and gender bias within the broad context of discrimination and not as a specific or separate problem. As we will see, this approach is reflected in the Act itself, where gender equality is not identified as a stand-alone target – a treatment that stands in stark contrast to UNESCO's recommendations and raises questions about whether this subsumption under general non-discrimination provisions adequately addresses the specific and multifaceted challenges of gender bias in AI. This pattern also reflects the EU's broader contemporary approach to gender equality in recent legal initiatives, where gender concerns are frequently integrated within general equality frameworks rather than being addressed through targeted mechanisms. The report addresses gender biases in the 'Algorithmic discrimination' section with reference to facial recognition systems, acknowledging that biases that occur for women may not occur for men due to data that 'might be unrepresentative, incomplete or contain historical biases'. According to the report, this concern is part of the general problem of biases in the existing data that AI depends on. The report acknowledges that use of discriminatory AI systems may lead to serious societal consequences whereby AI regenerates 'existing or create[es] new forms of structural discrimination and exclusion'.

The report also refers to gender equality concerns in the section called 'Requirements for trustworthy AI envisaged in the EU voluntary labelling scheme' (p. 41), where it explains certain policy decisions made in the AI Act. Accordingly, gender equality was one of the five requirements proposed by the European Parliament for high-risk systems. The Parliament's proposals during the legislative process included specific requirements addressing gender equality in high-risk AI systems, reflecting parliamentary concerns about the potential for AI to perpetuate gender discrimination. These proposals emerged from the Parliament's amendments to the Commission's original draft and sought to establish gender equality as an explicit requirement alongside other fundamental rights protections. The decision not to incorporate these proposals into the final Act represents a significant gap between parliamen-

tary advocacy for gender-responsive AI regulation and the adopted legislative framework. As stated explicitly in the report, 'it was decided not to include some of the [European Parliament] proposals or the High Level Expert Group on AI's principles as requirements […] because they were considered […] too vague for a legal act and too difficult to operationalize'. Certain other requirements proposed by the Parliament were not included on the grounds that they were already covered by other EU legal acts, such as the example of privacy and the GDPR. The report does not make such a claim for gender equality, implicitly admitting that there are no existing legal rules that would comprehensively cover this area in the AI context. The EU has also adopted the Directive on Violence against Women and Domestic Violence, which specifically criminalizes the non-consensual production of AI-generated or manipulated material depicting persons in sexually explicit activities (deepfakes), showing the EU's broader commitment to addressing gender-related AI harms. However, the impact assessment report does not refer to this Directive as legal grounds for ensuring gender equality in the context of AI systems. Instead, the report claims that this requirement would not be specific enough or would be too difficult to implement.

The AI Act itself contains few direct references to gender equality in the main text. While it refers to vulnerable persons or groups seven times, gender is not conceived as a factor of vulnerability. In the recitals, gender-related references are more frequent but still limited. While 'fundamental rights' appears 61 times and 'discrimination' 33 times, 'women' and 'gender' appear only two and four times respectively. Recital 27, which outlines the ethical principles for trustworthy AI, states that '[d]iversity, non-discrimination and fairness means that AI systems are developed and used in a way that includes diverse actors and promotes equal access, gender equality and cultural diversity, while avoiding discriminatory impacts and unfair biases'. Recital 48 refers to gender equality as a fundamental right protected under the EU Charter of Fundamental Rights, underlining that any violation of such a right would play an important role in classifying an AI system as high-risk. Recital 58 draws attention to the specific problem where AI systems are used to determine potential beneficiaries of public or private services and particularly the right to certain financial resources. It acknowledges that AI systems used for such purposes may lead to discriminatory results or 'may perpetuate historical patterns of discrimination', including gender biases; such consequences will be considered when assessing the risk level of AI systems. On the other hand, the term '(non-)discrimination' appears 16 times throughout the Act, and 'women' is mentioned twice, indicating that gender equality is primarily addressed within the broader non-discrimination framework rather than as a stand-alone concern.

In the main articles, the term 'fundamental rights' appears 45 times, while 'bias' or 'biases' appears nine times and 'discrimination' only twice. The term 'gender' is recorded just twice, with only one explicit reference to gender equality in Article 95, which deals with voluntary codes of conduct for non-high-risk AI systems. Al-

though the Act does not establish a specific target for gender equality or provide special prohibitions for gender biases directly, it includes provisions for bias audits and fundamental rights impact assessments that can help reduce gender biases and discriminatory risks in AI systems. However, critics note that while the Act aims to safeguard fundamental rights and address gender discrimination, it lacks comprehensive mechanisms specifically for gender-related issues and does not mandate fundamental rights impact assessments for all systems. It is therefore worth analysing various articles of the Act that may have indirect consequences for gender equality and examining how they have been received in academic discussions.

Article 5 of the AI Act establishes prohibitions on AI practices deemed unacceptable due to their potential to jeopardize safety and fundamental rights, explicitly banning systems such as social scoring and manipulative techniques targeting vulnerable individuals. While the provision prohibits biometric categorization systems in public spaces involving sensitive characteristics such as race and sexual orientation, it notably omits gender from this protected list, raising significant concerns about gender protection in contexts of social behaviour and performativity. In a comprehensive report penned for the Friedrich Ebert Stiftung, Karagianni (2025b) identifies a critical oversight in this approach to vulnerability in Article 5 of the Act, drawing attention to the concept of vulnerability as understood in both computer science and social sciences and highlighting how it particularly affects marginalized groups. Despite recommendations from the European Data Protection Board to include gender as a sensitive category, this has not been integrated into the AI Act. Furthermore, as indicated above, the UNESCO recommendations also emphasize the importance of making gender equality a specific target within vulnerable groups (UNESCO, 2020). This omission by the AI Act represents a fundamental gap in ensuring gender equality in AI systems and underscores the need for an intersectional approach, as outlined by UNESCO, that acknowledges the complex layers of discrimination inherent in AI technologies. The failure to recognize gender as a sensitive characteristic leaves women and gender minorities vulnerable to discriminatory treatment by AI systems operating in public spaces.

Data governance is one of the most critical areas for addressing gender equality concerns. The data governance requirements in the AI Act's Article 10 will be operationalized through the future European standard on 'Data and data governance', which aims to develop specifications for adequate data governance and data management procedures for AI system providers. The standard has a twofold purpose: first, to establish specifications for data governance and management procedures focusing on data generation, collection, preparation operations, design choices, and procedures for detecting and addressing biases; and second, to provide specifications on quality aspects of the datasets used to train, validate, and test AI systems, including requirements for representativeness, relevance, completeness, and correctness. The 'gender data gap' within this framework is crucial: datasets often suffer from being

non-representative, incomplete, and incorrect due to the digital gender divide and prevailing gender stereotypes. Lütz (2024) argues that this standard would benefit significantly from incorporating gender equality expertise and ensuring women's involvement in both its development and implementation phases to enable diverse perspectives and identify potential pitfalls in data governance practices. According to Lütz, the doctrine and institutional reports have clearly identified design choices and datasets as potential entry points for gender biases and discrimination throughout the algorithmic development process, from data collection and generation to the modification and preparation of training datasets. Given that bias detection and subsequent addressing of gender biases serve as crucial tools for achieving gender equality, clear guidance is essential for both companies and enforcement authorities.

Article 27 outlines the Fundamental Rights Impact Assessment (FRIA) as a solution for protecting fundamental rights endangered by high-risk AI systems, working alongside the risk management system detailed in Article 9. However, questions arise regarding their adequacy in preventing gender-based discrimination and promoting gender equality within AI contexts. While these represent novel measures in AI regulation, risk management and impact assessments are not new constructs in technology regulation, having historically emerged to address uncertainties associated with technological advancements.

The existing literature lacks comprehensive analysis of the differences between and practical applications of risk management systems and FRIAs, particularly in AI contexts. Defining what constitutes a risk to rights such as non-discrimination involves multiple conceptualizations, complicating risk measurement as a subjective process often influenced by gendered assumptions. The relationship between risk management systems, FRIAs, and gender impact assessments, which specifically address impacts on gender equality, remains unclear and requires clarification. Karagianni argues that incorporating gender impact assessments into risk management systems and fundamental rights impact assessments is essential, reinforcing the principle that 'women's rights are human rights' (Karagianni, 2025b). Without this integration, these assessment tools risk protecting only the rights of a standard, liberal legal persona, typically male, white, and able-bodied. This claim is also parallel to the recommendations of UNESCO on the responsibilities of governments to establish adequate monitoring and assessment mechanisms. Gender impact assessments highlight how development initiatives affect individuals differently based on their gender, and aim to uncover disparities caused by entrenched structural inequalities. Examples include the identification of potential gender-based impacts, assessment of whether AI systems reinforce existing inequalities, examination of intersectional factors, consideration of gender-specific rights under international treaties, and collection of gender-disaggregated data to understand different experiences and needs.

For general-purpose AI systems under Article 51 and post-release obligations under Article 26, while the Act mandates ongoing monitoring to detect evolv-

ing biases, it relies heavily on self-regulation and lacks robust redress mechanisms (Karagianni, 2025a). This is particularly problematic because gender bias in AI disproportionately harms marginalized communities who often lack institutional power to demand accountability. The Act provides no clear pathways for individuals affected by algorithmic discrimination to seek justice, such as women rejected by biased AI hiring systems.

The standardization process established in Articles 40 and 41, while creating important technical standards through bodies like European Committee for Standardization (CEN), European Committee for Electrotechnical Standardization (CENELEC) and European Telecommunications Standards Institute (ETSI), is criticized for lacking mandatory intersectional gender audits and diverse AI development teams (Lütz, 2024). The AI standardization process outlined in Article 40 is essential for establishing comprehensive guidelines, technical specifications, and best practices that ensure AI systems are safe, reliable, transparent, and ethically designed. This standardization involves the development and implementation of norms and technical standards by various entities, including European standards organizations, national standards bodies, and the European Commission, working together to establish frameworks regulating AI with a focus on human-centred AI, security, privacy, and data governance. The standardization process faces significant challenges regarding inclusive participation. While the European Commission has emphasized the need to include representatives from various sectors and organizations, achieving consensus on important issues has proven difficult. Karagianni (2025b) emphasizes the importance of explainability and accountability within AI systems as critical to upholding fundamental rights. There is also substantial risk of tokenism, where the involvement of diverse stakeholders remains superficial and fails to result in substantive changes promoting gender equity. This challenge is exacerbated by the AI standardization process being predominantly shaped by powerful corporations and governments, which may obstruct genuine feminist efforts to cultivate inclusivity and equity in AI development and regulation.

High-risk AI systems are mandated to undergo conformity assessments during their evaluation stage to ensure adherence to established safety and ethical standards before market release. This process verifies system compliance with necessary requirements and creates a comprehensive regulatory framework for such systems. Article 43 works in conjunction with Article 6 to establish governance structures aimed at overseeing compliance and enforcement, promoting responsible AI development while safeguarding individual rights and interests.

From a feminist perspective, AI conformity assessment must address gender bias, inclusivity, and power structures, particularly given systemic inequalities that may be perpetuated if assessments lack an intersectional lens. A prominent feminist concern is the reinforcement of gender bias through biased algorithms and data, as AI systems often rely on historical data reflecting existing social inequalities. Consequently,

conformity assessments should require comprehensive bias audits extending beyond identifying overt discrimination to pinpointing subtle structural biases against women, particularly women of colour, LGBTQIA+ individuals, and other marginalized groups. Intersectional data analysis in conformity assessments is essential, as gender bias should not be evaluated in isolation (UNESCO, 2020). Assessments must consider how gender intersects with race, class, disability, and other identity factors to ensure AI systems do not disproportionately harm marginalized communities. The assessment process should involve diverse teams reflecting a range of genders, races, and social backgrounds to ensure AI systems are scrutinized through multiple lenses, minimizing bias and enhancing fairness (Karagianni, 2025b).

The Council of Europe Framework Convention on Artificial Intelligence provides an important comparative perspective on how gender equality can be integrated into international AI governance. As the first legally binding international treaty on AI, the Convention establishes equality and non-discrimination as fundamental principles that must be respected throughout the lifecycle of AI systems. The Convention's approach has prompted scholarly analysis of its implications for gender equality, with researchers like Bartoletti and Xenidis (2023) examining how its provisions address discrimination and equality concerns. The EU's participation in developing this Convention reflects the broader European commitment to human rights-based AI governance, yet the relationship between the Convention's equality provisions and the AI Act's treatment of gender remains an area requiring further harmonization and clarity.

The policy and regulatory landscape reveals a fundamental tension between aspirational frameworks and practical implementation in addressing gender bias in AI systems. While UNESCO's recommendations provide a comprehensive blueprint for integrating gender equality as a central principle in AI governance, emphasizing meaningful participation, intersectionality, and transformative approaches that go beyond harm prevention, the EU AI Act's treatment of gender issues remains fragmented and inadequate. Despite being the world's first comprehensive AI regulation, the Act's failure to establish gender equality as a stand-alone principle, its omission of gender from protected characteristics in key provisions, and its reliance on general non-discrimination frameworks rather than targeted gender-specific mechanisms highlight the significant gap between recognition of the problem and regulatory solutions. This treatment reflects a broader pattern in the EU's recent legal initiatives, where gender equality concerns are frequently subsumed within general equality and diversity frameworks rather than receiving dedicated attention. The EU's exclusive focus on avoiding harm, to the exclusion of UNESCO's other two dimensions – increasing visibility and contributing to empowerment – further limits the transformative potential of AI regulation for advancing gender equality. This disparity underscores the urgent need for more deliberate and comprehensive integration of gender equality considerations into AI governance frameworks, moving beyond to-

kenistic inclusion toward substantive transformation of how AI systems are developed, deployed, and monitored.

Conclusions

The analysis of gender bias in AI systems and regulatory responses reveals a significant disconnect between the comprehensive frameworks proposed by international organizations and the practical implementation found in existing legislation. While the UNESCO recommendations provide a holistic, transformative approach to integrating gender equality into AI governance, the European Union's AI Act, despite being groundbreaking in its scope, falls short of adequately addressing the complex challenges of gender discrimination in artificial intelligence systems.

The UNESCO framework's emphasis on treating gender equality as a stand-alone principle rather than subsuming it under broader categories of bias or discrimination stands in stark contrast to the EU AI Act's approach. Where UNESCO calls for gender equality to be positioned prominently within frameworks with clear implementation pathways, the EU Act relegates gender considerations to occasional mentions within broader non-discrimination provisions. This fundamental difference reflects deeper philosophical divides about whether gender bias requires specialized attention or can be adequately addressed through general fairness mechanisms. The EU's treatment of gender equality within general non-discrimination frameworks mirrors a broader tendency in the Union's recent legal initiatives, suggesting systemic challenges in recognizing and addressing the specific dimensions of gender inequality in technological contexts.

Most critically, the UNESCO recommendations advocate for a three-dimensional approach – avoiding harm, increasing visibility, and contributing to empowerment – that goes far beyond the EU Act's focus primarily on harm prevention. The EU's exclusive focus on avoiding harm, without incorporating mechanisms for increasing women's visibility in AI development or leveraging AI's potential for empowerment, represents a missed opportunity for transformative change. While the EU Act establishes important prohibitions and risk management requirements, it lacks the proactive mechanisms necessary to leverage AI's potential for advancing gender equality. The absence of mandatory gender impact assessments, the omission of gender from sensitive characteristics in biometric categorization prohibitions, and the limited pathways for redress all highlight the Act's reactive rather than transformative approach to gender equality. This narrow focus fails to address why gender equality was excluded from the final regulatory framework despite being proposed by the European Parliament, suggesting that concerns about operationalization and vagueness may have overshadowed the fundamental importance of targeted gender equality provisions.

The standardization processes outlined in the EU Act present both opportunities and risks for gender equality. While these processes could potentially incorporate gender expertise and diverse perspectives, the current framework relies heavily on self-regulation and lacks mandatory requirements for intersectional gender audits or diverse development teams. This contrasts sharply with UNESCO's emphasis on the meaningful participation of gender equality experts throughout the entire lifecycle of AI governance frameworks. The meaningful participation that UNESCO envisions – involving gender experts and women in formulation, interpretation, application, and monitoring – requires institutional mechanisms that recognize and value their contributions, ensure their voices shape decisions rather than merely being consulted, and create pathways for their insights to influence technical standards and implementation practices. The conformity assessment mechanisms in the EU Act, while innovative, require significant enhancement to address structural gender biases effectively. The current assessment framework lacks the intersectional lens that UNESCO identifies as essential for understanding how gender intersects with race, class, disability, and other identity factors. Without comprehensive bias audits that extend beyond identifying overt discrimination to uncover subtle structural biases, these assessments risk perpetuating existing inequalities while providing a veneer of compliance. The Council of Europe Framework Convention on Artificial Intelligence offers an important complementary perspective, establishing equality and non-discrimination as fundamental principles in the first legally binding international treaty on AI. However, the relationship between the Convention's approach and the EU Act's provisions requires further examination to ensure the coherent and comprehensive protection of gender equality across European AI governance frameworks.

Moving forward, the implementation of the EU AI Act presents a critical opportunity to bridge the gap between aspirational principles and regulatory practice. As the Act's provisions come into force through 2026, there is an urgent need to incorporate gender equality expertise into the development of technical standards, ensure the meaningful participation of diverse stakeholders in governance structures, and establish robust monitoring mechanisms that centre the voices of affected women and marginalized communities. The implementation phase must address why the European Parliament's proposals for explicit gender equality requirements were deemed too vague or difficult to operationalize, and explore concrete mechanisms for translating gender equality principles into enforceable standards. Only through such comprehensive integration can AI regulation move beyond protecting the status quo to actively promoting gender equality in the digital age. The stakes are too high, and the potential for both harm and advancement too great, to accept anything less than a truly transformative approach to gender equality in AI governance.

REFERENCES

Ahn, J., Kim, J., & Sung, Y. (2022). The effect of gender stereotypes on artificial intelligence recommendations. *Journal of Business Research*, *141*, 50–59.

Andrews, L., & Bucher, H. (2022). Automating discrimination: AI hiring practices and gender inequality. *Cardozo Law Review*, *44*, 145–178.

Bartoletti, I., & Xenidis, R. (2023). The Council of Europe's Framework Convention on Artificial Intelligence: Equality and non-discrimination perspectives. *European Equality Law Review*, *1*, 56–72.

Buolamwini, J., & Gebru, T. (2018). Gender shades: Intersectional accuracy disparities in commercial gender classification. *Conference on Fairness, Accountability and Transparency*, *81*, 77–91.

Domnich, A., & Anbarjafari, G. (2021). Responsible AI: Gender bias assessment in emotion recognition. *arXiv preprint*. arXiv:2103.11436.

Fountain, J. E. (2004). *Building the virtual state: Information technology and institutional change*. Brookings Institution Press.

Karagianni, A. (2025a). Gender in a stereo-(gender)typical EU AI law: A feminist reading of the AI Act. *Cambridge Forum on AI: Law and Governance*, *1*(e25), 1–18.

Karagianni, A. (2025b). *The EU Artificial Intelligence Act through a gender lens*. Friedrich-Ebert-Stiftung e.V. https://library.fes.de/pdf-files/bueros/bruessel/21887–20250304.pdf

Lau, P. L. (2023). AI gender biases in women's healthcare: Perspectives from the United Kingdom and the European legal space. In E. Gill-Pedro & A. Moberg (Eds.), *YSEC yearbook of socio-economic constitutions 2023: Law and the governance of artificial intelligence* (pp. 247–274).

Lütz, F. (2024). The AI Act, gender equality and non-discrimination: What role for the AI office? *ERA Forum*, *25*, 79–95.

Manasi, A., Panchanadeswaran, S., Sours, E., & Lee, S. J. (2022). Mirroring the bias: Gender and artificial intelligence. *Gender, Technology and Development*, *26*(3), 295–305.

O'Connor, S., & Liu, H. (2024). Gender bias perpetuation and mitigation in AI technologies: Challenges and opportunities. *AI & Society*, *39*, 2045–2057.

Orlikowski, W. J. (1992). The duality of technology: Rethinking the concept of technology in organizations. *Organization Science*, *3*(3), 398–427.

Otis, N. G., Delecourt, S., Cranney, K., & Koning, R. (2024). *Global evidence on gender gaps and generative AI* [Working paper 25–023]. Harvard Business School.

UN Women. (2025, 5 February). *How AI reinforces gender bias – and what we can do about it: Interview with Zinnya del Villar on AI gender bias and creating inclusive technology*. https://www.unwomen.org/en/news-stories/interview/2025/02/how-ai-reinforces-gender-bias-and-what-we-can-do-about-it

UNESCO. (2020). *Artificial intelligence and gender equality: Key findings of UNESCO's global dialogue*. https://unesdoc.unesco.org/ark:/48223/pf0000374174/PDF/374174eng.pdf.multi

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

sciendo

DOI: 10.15290/bsp.2026.31.01.09

Received: 26.06.2025
Accepted: 08.01.2026

Michal Petr
Palacky University, Olomouc, Czech Republic
michal.petr@upol.cz
ORCID ID: 0000–0001–6495–4530

The Digital Markets Act: What Have We Learned after the First Years of Its Application?

Abstract: The Digital Markets Act (DMA) became applicable in May 2023. It is completely new piece of legislation affecting a sector which has not been subject to any specific regulation before, and it introduced brand new concepts aimed at protecting the digital rights of consumers and business entities alike. What have we learned after the first years of its full application? Has the European Commission's practice clarified the concepts that were disputed? Did it have any measurable effects on the markets? Has it brought any specific improvement in consumers' digital rights? This paper re-interprets the DMA in the light of recent case law, evaluates its practical impact so far and tries to predict how its future application might affect the protection of digital rights.

Keywords: core platform services, Digital Markets Act, gatekeepers, regulatory dialogue

Introduction

The economic significance of digital markets is enormous, and it continues to grow. Even before the COVID-19 pandemic, which enabled an unprecedented expansion of some digital services, it was estimated that the digital economy stands for 15.5% of world GDP (OECD, 2021, p. 6). It is generally accepted that markets with undistorted competition are the most effective ones, but unfortunately, digital markets are prone to competition concerns. Thus the European Commission has argued that '[u]nfair practices and lack of contestability lead to inefficient outcomes in the digital sector in terms of higher prices, lower quality, as well as less choice and innovation to the detriment of European consumers' (European Commission, 2020a). As

a consequence, a large number of reports and policy papers in recent years have argued that the key features of digital platform markets present the hallmarks of market failure, warranting regulatory action, in addition to *ex post* antitrust enforcement, in view of their significant influence on markets and society at large (OECD, 2021, p. 6).

As a 'European' solution to this problem, the Digital Markets Act (DMA) was adopted in 2022 (European Parliament and Council of the EU, 2022a). In the last two years, its provisions have been gradually entering into force, and it is today possible to evaluate the first experiences with its application in practice. The DMA is not simply a new piece of regulation, but also, as I will argue in this paper, a new regulatory approach to market power, based, among other characteristics, on the 'regulatory dialogue' between the 'gatekeepers' and the Commission. Interpretation of the DMA is therefore challenging and cannot be definitive without a review of actual cases. It has not been universally endorsed, and even its basic principles have been subject to criticism (Akaman, 2022 Gönenç et al., 2022; Monti, 2021). Without revisiting this robust debate, this article is focused on the actual application of the DMA.

The DMA is basically applied in two steps: identification ('designation') of its addressees (the 'gatekeepers'), followed by monitoring and enforcing their compliance with the DMA-imposed obligations. As of today, the designation process has been significantly clarified by the Commission and the General Court of the European Union. The process of compliance has already started, but the number of decisions is limited, and none has reached the level of court review; notwithstanding this, some trends may already be identified.

The aim of this paper is to analyse the experience of the application of the DMA so far and to answer the following questions: (1) To what extent has the notion of the gatekeeper been clarified? (2) Does the 'regulatory dialogue' help with effective compliance and enforcement? (3) Do the gatekeepers comply with the DMA-imposed obligations? (4) Does the DMA live up to expectations? In order to answer these questions, I will first reiterate the reasons why the DMA was adopted as a specific piece of legislation, its objectives and the expectations it has raised (section 1). Thereafter, I will briefly introduce the process of the application of the DMA, as it was foreseen by the text of the regulation itself, as well as by the commentaries published before it actually entered into force (section 2); this will be followed by two sections dedicated to the practice so far on the designation of gatekeepers (section 3) and their compliance with the DMA (section 4). In so doing, I will conduct a review of the academic literature discussing these issues and will perform a qualitative analysis of the Commission's decisions based on the DMA, as well as the General Court's judgments reviewing them. All decisions taken before 31 March 2025 will be taken into account.

1. Reasons for adopting the DMA and its goals

In this section, I will summarise the particular characteristics of digital markets, argue why a distinctive regulation is needed with regard to them and outline the DMA's goals and means to achieve them.

1.1. Specific features of digital competition

Competition-related issues in digital markets are typically associated with 'platforms' (Evans, 2003), which may be characterised as undertakings providing services to different groups of interconnected consumers (OECD, 2022, p. 10); platforms are frequently multi-sided, meaning that a platform is active in a market where it sells different products to different groups of consumers, while the demand from one group of consumers depends on the demand from other groups. For example, a digital content platform may feature content creators on one side, viewers of content on the other and advertisers on another.

From the point of view of competition, several characteristics of platforms stand out. First, they are characterised by an extreme return to scale, network externalities and the role of data (Montjoye et al., 2019, p. 2). They are typically disruptive, creating new markets and replacing traditional ones (Cohen, 2018, p. 19). Second, they tend to be multi-sided, and the services of the platforms are frequently not paid for by the final consumers. Without having a price, platforms generally compete on quality and innovation (Jenny, 2021, p. 3) and for the attention of consumers rather than directly for their money (Newman, 2021). At the same time, consumer choice is limited by network effects: the quality of a platform is frequently defined by the number of people using it, which may dissuade consumers from switching. And third, platforms tend to form 'ecosystems' (Montjoye et al., 2019, p. 33), which transform the competition from being at a platform level to an ecosystem one. As a consequence of these characteristics, the platforms typically wield significant market power, and from the competition point of view, the markets in which they operate tend not to be sufficiently competitive.

1.2. The need for specific regulation

Can these specifics of digital markets be effectively addressed by traditional competition law, in particular Article 102 TFEU? It has been argued that the enforcement of this article is faced with two principal challenges in digital markets (Morbel, 2023, p. 208): first, the intervention threshold is relatively high. In the case of abuse of dominance, it is necessary to define the relative market and assess the market power of the undertaking concerned in order to decide whether it is in a dominant position, which is in itself very demanding (Solek, 2021, p. 595). In addition to this, it is necessary to substantiate the negative effects on competition of the conduct in question. This amounts to very long proceedings, meaning that any eventual intervention may

not be sufficiently timely. Second, it may be difficult to devise appropriate remedies for market failure in proceedings that are concluded by prohibition of the anticompetitive conduct.

Such problems are not only specific to digital markets. Indeed, the Commission launched an initiative in 2020 to adopt the 'New Competition Tool', enabling it to impose remedies without finding an infringement of competition law (Vesterdorf & Fountoukalos, 2021, p. 284). This project has nonetheless been abandoned; instead, a consensus began to form in the EU that a new regulatory approach specifically for digital markets might be necessary.[1] In 2019, the Commission published the study *Competition Policy for the Digital Era*, concluding that it is necessary to promote competition both for the market (i.e. enabling other platforms to acquire a critical mass of users) and in the market (i.e. preventing abusive behaviour by the dominant platform) (Montjoye et al., 2019, p. 6). At the same time, it conceded that a vigorous enforcement of competition law in digital markets may not be enough, as '[i]n some areas, […] a regulatory regime may be needed in the longer run' (Montjoye et al., 2019, p. 126). This thinking was translated into the adoption of the DMA in 2022. The DMA's aim is to pragmatically recalibrate the relationship between the enforcer and undertakings in the relevant markets (Tyagi et al., 2024, p. 43). It is meant not only to enable 'turbocharged application of Article 102 TFEU' (Monti, 2021, p. 90), but is a new instrument, rather than an element of competition law (Morbel, 2023, p. 208).

It is not the goal of this paper to discuss whether the DMA is part of competition law *stricto sensu* or a specific regulation of digital markets. This issue has been thoroughly discussed elsewhere (Tyagi et al., 2024, p. 47) and is ultimately not decisive for our further thoughts. In my opinion, the regulatory, *ex ante* character of the DMA prevails nonetheless (Petr, 2024, p. 158), putting it outside of competition law *stricto sensu*. This places it among a number of recently adopted legislative initiatives targeting different aspects of digital markets. The Digital Services Act (European Parliament and Council of the EU, 2022b), adopted in parallel with the DMA, in particular protects consumers by striving to achieve a safe, predictable and trusted online environment for platforms. Given the crucial importance of data for digital markets, the original General Data Protection Regulation (European Parliament and Council of the EU, 2016), protecting personal data, was complemented by the Data Act (European Parliament and Council of the EU, 2023), which focuses among other things on switching, interoperability and data transfers, and by the Data Governance Act (European Parliament and Council of the EU, 2022c).

Conversely, the DMA brings a general regulation to the operation of platforms, and strives to secure contestable and fair markets in the digital sector (as will be discussed in detail below). In this regard, it is in line with general competition law, which

1 For a summary of the debate, see e.g. OECD, 2021. For an overview of relevant literature, see e.g. Botta, 2021, p. 501.

also provides a basic regulatory framework for the protection (or even existence) of competition, not specific regulation on the individual business activities of the undertakings concerned. In the following section, I will concentrate on the DMA's objectives and the regulatory means employed to achieve them.

1.3. Objectives and tools of the DMA

The DMA's purpose 'is to contribute to the proper functioning of the internal market by laying down harmonised rules ensuring for all businesses, contestable and fair markets in the digital sector across the Union where gatekeepers are present, to the benefit of business users and end users' (DMA, Art. 1(1)). It thus seems to be pursuing two objectives: first, that the markets become and remain contestable, and second, that the functioning of these markets is fair (DMA, Recitals 4–8; for detail, see e.g. Ibáñez-Colomo, 2021, p. 563). The approach of the DMA to these two goals resembles the regulation of unfair business practices rather than traditional competition law. It is based on a premise that the economic power of the gatekeepers may lead 'to serious imbalances in bargaining power and, consequently, to unfair practices and conditions for business users, as well as for end users of core platform services provided by gatekeepers, to the detriment of prices, quality, fair competition, choice and innovation in the digital sector' (DMA, Recital 4).

The DMA imposes specific obligations on the gatekeepers, aimed at restraining them in a systematic manner. It focuses on three broad categories of activities by providers of platform services (Ibáñez-Colomo, 2021, p. 563): the entrenching and strengthening of the position of a gatekeeper on a specific platform, the leveraging of market power from the platform to adjacent activities, and the exploitation of the position of the gatekeeper within the platform.

The DMA imposes *ex ante* obligations on the gatekeepers, while not requiring the enforcers to substantiate the significant market power of the gatekeepers or the negative effects of their conduct on competition. There is no need for any specific assessment of the actual or potential effects on competition of the conduct in question, and the defence of efficiency is not permissible (Bania & Geradin, 2025, p. 246). This regulatory approach aims at facilitating fast and effective enforcement of these obligations (Morbel, 2023, p. 209). Whereas the application of traditional competition law in digital markets takes years,[2] the gatekeepers need to comply with the DMA immediately. In this sense, it is indeed a 'genuine regulatory law' (Schmidt & Hübener, 2023, p. 42).

The DMA may be regarded as an example of a new approach to problems with competition in dynamic markets, characterised in particular by its asymmetric scope, its being proactive, and regulation based on dialogue rather than strict rules (Tyagi

2 For example, the investigation in the *Google Shopping* case was formally initiated in 2010, the decision was issued in 2017, the General Court decided in 2021 and the Court of Justice decided in 2024, after almost 15 years since the opening of the case.

et al., 2024, p. 47). By asymmetric scope, I mean that unlike 'traditional' competition law, which is universally applicable to all businesses in all the relevant markets, the DMA is only applied to a few specific undertakings – gatekeepers, active in several specific digital markets – the platform services (these concepts will be discussed in detail in section 2.1). By proactive, I mean that the DMA is based on *ex ante* rather than *ex post* regulation. Whereas 'traditional' competition law remedies market distortions caused by specific infringements of that law, the DMA imposes obligations on undertakings that have not infringed any specific legal duty. The nature of these obligations is dialogue-based: the specific obligations of the gatekeeper are not prescribed by the DMA itself, which defines them only in rather general terms, but on the basis of the 'regulatory dialogue' (discussed below in section 4.1). This feature of the DMA is sometimes referred to as 'opacity by design' (Tyagi et al., 2024, p. 51).

2. Application of the DMA

The DMA is applied in several consecutive steps. The first is the identification (designation) of the gatekeepers; the second is securing compliance with obligations, imposed on the gatekeepers by the Act. Both these procedures will be outlined in this section, followed by discussion of their actual application in sections 3 and 4. Finally, if the obligations are not fulfilled, a sanction procedure may follow. As there had been no practical experience with this when this article was finalised, the sanction procedure will be described only briefly.

2.1. Designation of gatekeepers

The gatekeepers are the providers of core platform services (DMA, Art. 2(1)). These services are defined by an exhaustive list of activities, in which the market position of the providers is clearly visible (Morbel, 2023, p. 210).[3] It is unfortunate that the DMA does not provide a general definition of core platform services; this may complicate its interpretation, as well as the possible future expansion of the list (Schmidt & Hübener, 2023, p. 25). The general characteristics are nonetheless discernible from the DMA's recitals: they include 'extreme' economies of scale, 'very strong' network effects, the 'multisidedness' of the platform, a 'significant degree' of user dependence, lock-in effects, vertical integration of the providers and data-driven advantages (DMA, Recital 2). Indeed, these are the characteristics of a platform economy, as discussed in the pre-

3 According to Article 2(2), DMA, the core platform services consist of: online intermediation services; online search engines; online social networking services; video-sharing platform services; number-independent interpersonal communications services; operating systems; web browsers; virtual assistants; cloud computing services; and online advertising services, by an undertaking that provides any of these core platform services.

vious section. The current list of core platform services is mostly based on experience with the application of competition law (European Commission, 2020b, p. 37).

The list is exhaustive, so as long as a particular service is not on it, its provider cannot be a gatekeeper. The list may nonetheless be expanded by a regular legislative procedure, initiated by a Commission proposal based on a market investigation (DMA, Art. 19). Artificial intelligence systems, such as OpenAI's ChatGPT, are currently being discussed as potential candidates (Martínez, 2025, p. 4).

Not every provider of a core platform service is a gatekeeper. In order to qualify, three conditions need to be met: the undertaking concerned must (1) have a significant impact on the internal market; (2) provide a core platform service which is an important gateway for business users to reach end users; and (3) enjoy in its operations an entrenched and durable position; alternatively, it must be foreseeable that it will enjoy such a position in the near future (DMA, Art. 3(1)). These conditions are presumed to be satisfied if the following quantitative criteria are cumulatively met: (1) the undertaking provides the same core platform service in at least three Member States and achieves an annual EU turnover equal to or above EUR 7.5 billion in each of the last three financial years (or its average market capitalisation amounted to at least EUR 75 billion in the last financial year); (2) the core platform service had at least 45 million monthly active end users in the EU and at least 10,000 yearly active business users in the last financial year; and (3) these minimum numbers of users were met in each of the last three financial years (DMA, Art. 3(2)).

An undertaking does not become a gatekeeper per se; it needs to be 'designated' as such by the Commission. First, if it meets the quantitative criteria described above, it needs to make a notification to the Commission (DMA, Art. 3(3)). The details are set in the DMA Implementing Regulation (European Commission, 2023, Annex I). The deadline for the first notifications after the DMA entered into force was July 2023 (DMA, Art. 54). Second, following the notification, the Commission is obliged to issue a designation decision within 45 working days; as a matter of principle, it designates as a gatekeeper an undertaking fulfilling the quantitative criteria (DMA, Art. 3(4)). The businesses concerned may nonetheless rebut the presumption. Sufficiently substantiated arguments need to be presented with the notification (DMA, Art. 3(5)). If the Commission considers that the undertaking's arguments are sufficiently substantiated to manifestly call into question the qualitative presumptions, it will open a market investigation according to Article 17(3) DMA (DMA, Art. 3(5)), which needs to be finished within five months (DMA, Art. 17(3)). Finally, even when the quantitative criteria are not fulfilled, an undertaking may be designated a gatekeeper if, following a market investigation not exceeding 12 months (DMA, Art. 17(1)), the Commission can demonstrate that the qualitative criteria are met (DMA, Art. 3(8)). The Commission shall regularly, and at least every three years, review whether the gatekeepers continue to satisfy the qualitative requirements laid down in Article 3(1) DMA. Understandably, such a review has not yet taken place.

2.2. Obligations of the gatekeepers

Once designated, a number of obligations apply to the gatekeepers. Unlike in the case of abuse of dominance, where the prohibition according to Article 102 TFEU is very broad ('any abuse of a dominant position shall be prohibited'), the DMA provides an exhaustive list of specific duties and obligations. Unfortunately, these are not structured in any way, and there is no reference to their objective (fairness or contestability), theme or a theory of harm (Bania & Geradin, 2025, p. 127). Attempts to create a 'taxonomy' (e.g. Ibáñez-Colomo, 2021; Morbel, 2023) have not been conclusive (Bania & Geradin, 2025, p. 127). The only distinction, contained in the DMA itself, is the different regulatory approach to the obligations under Article 5 DMA, commonly referred to as 'self-executing' (Morbel, 2023, p. 211),[4] and under Articles 6 and 7 DMA, which are 'susceptible of being further specified' within a 'regulatory dialogue procedure' (DMA, Art. 8(3)).[5]

It is not the goal of this paper to go into details on the specific obligations contained in the DMA. I have discussed their general regulatory characteristics above in section 1.3. At this point, I would only like to recall the concept of 'opacity by design', which indicates that the specific content of these obligations is in itself rather unpredictable. Therefore even the self-executing obligations, which were supposed to be clear-cut and not requiring any further clarification, seem to be 'not sufficiently clear and precise to qualify as self-executing' (Bania & Geradin, 2025, p. 170). I will discuss this in section 4, in connection with the experience with compliance.

The gatekeepers are obliged to comply with both the 'self-executing' and 'to-be-specified' obligations with respect to each of its core platform services listed in the designation decision (DMA, Art. 8(1)), within six months of the designation (DMA, Art. 3(10)). Within this timeframe, the gatekeepers need to provide the Commission with a report describing in a detailed and transparent manner the measures that have been implemented to ensure compliance (the compliance report) (DMA, Art. 11(1)). Compliance reports need to be updated at least annually (DMA, Art. 11(2)), and non-confidential versions of them are available online.[6]

The gatekeepers also need to introduce a 'compliance function', i.e. one or more compliance officers, including the head of the compliance function (DMA, Art. 28(1)). The compliance function needs to be endowed with sufficient authority, stat-

4 Even though it may be argued that all the obligations contained in the DMA are self-executing (Schmidt & Hübener, 2023, p. 43), as they are all immediately binding on the gatekeepers, the existence of the regulatory dialogue procedure (see below) clearly distinguishes the two categories of obligations.

5 The DMA only uses the characteristic of 'susceptible of being further specified' in the case of Article 6. The regulatory dialogue procedure according to Article 8(3) DMA nonetheless refers to both Articles 6 and 7 DMA.

6 A dedicated webpage is accessible at https://digital-markets-act-cases.ec.europa.eu/reports/compliance-reports.

ure and resources, as well as access to the management body of the gatekeeper (DMA, Art. 28(2)). The head of the compliance function shall report directly to the management body and may raise concerns or warn that body where risks of non-compliance arise (DMA, Art. 28(4)). The Commission conformed in its first annual report that all the gatekeepers established the compliance function in line with the DMA (European Commission, 2024, para. 39).

In order to achieve compliance with the 'to-be-specified' obligations, a 'regulatory dialogue' procedure may be initiated. A gatekeeper may thus request the Commission to engage in a process to determine whether the measures that the gatekeeper intends to implement ensure compliance with Articles 6 and 7 and are effective in achieving their objective in the gatekeeper's specific circumstances.[7] The Commission shall have discretion in deciding whether to engage in such a process, respecting the principles of equal treatment, proportionality and good administration (DMA, Art. 11(3)). The Commission may also open such a procedure on its own initiative (DMA, Art. 11(2)). Within six months of opening the specification procedure, the Commission needs to adopt a decision, detailing the measures that the gatekeeper is to implement in order to effectively comply with its obligations (DMA, Art. 11(2)). Surprisingly, the procedure of regulatory dialogue has not yet been used (see below, section 4.1).

Compliance with the obligations prescribed by the DMA needs to be full and effective. In order to achieve this goal, the DMA provides for 'anti-circumvention rules', according to which the gatekeeper shall not engage in any behaviour that undermines effective compliance with the DMA obligations, regardless of whether that behaviour is of a contractual, commercial, technical or any other nature, or consists in the use of behavioural techniques or interface design (DMA, Art. 13(4)). If the gatekeeper circumvents or attempts to circumvent its obligations, the Commission may open proceedings and ultimately impose specific obligations in accordance with Article 8(2) DMA (DMA, Art. 13(7)). Such procedures have already been initiated, as will be discussed in section 4 below.

If non-compliance with the DMA is suspected, the Commission may open an official investigation (DMA, Art. 29(1)); a decision is to be adopted within 12 months (DMA, Art. 29(2)). In a decision finding non-compliance, the Commission may impose a fine of up to 10% of the annual global turnover of the gatekeeper concerned (DMA, Art. 30). The first non-compliance proceedings will be discussed in section 4.2 below. The Commission may even open a market investigation into systematic non-compliance (DMA, Art. 19); however, this provision has not yet been used.

In addition to the obligations outlined above, the gatekeepers must also inform the Commission of any intended concentrations, as defined by the Merger Regula-

7 The fact that this provision does not apply to the 'self-executing' obligations under Article 5 DMA has been criticised. See e.g Bania & Geradin, 2025, p. 243.

tion (Council of the EU, 2004, Art. 3), where the merging entities or the target of concentration provide core platform services or any other services in the digital sector or enable the collection of data, irrespective of whether it is notifiable to the Commission under that regulation or to a competent national competition authority under national merger rules (DMA, Art. 14). By the end of March 2025, 17 concentrations were notified by the gatekeepers.[8] A gatekeeper shall also submit to the Commission an independently audited description of any techniques for the profiling of consumers that the gatekeeper applies to or across its core platform services listed in the designation decision within six months after its designation (DMA, Art. 15).

These specific obligations will not be discussed further in this paper. Instead, the next two sections will be devoted to the first experiences the application of the DMA has brought so far, concerning both the designation of the gatekeepers (section 3) and the monitoring of their compliance (section 4).

3. The gatekeepers

By the end of 2024, the Commission had designated seven gatekeepers in relation to 24 core platform services.[9] On 3 July 2023, the Commission received the first notifications from seven undertakings: Alphabet, Amazon, Apple, ByteDance, Meta, Microsoft and Samsung (European Commission, July 2023). Following the notifications, the Commission designated six gatekeepers on 6 September 2023 (Alphabet, Amazon, Apple, ByteDance, Meta, Microsoft) with respect to 22 core platform services. Samsung, despite meeting the quantitative criteria, was not among them (European Commission, 6 September 2023).

Three of the designated gatekeepers (Apple, ByteDance and Meta) filed an action for annulment against the designation decisions. While two of these cases are still pending, ByteDance's action has already been dismissed; this judgment has been appealed to the Court of Justice, which had not decided by the end of March 2025.[10] I will discuss the General Court's judgment in more detail below.

The gatekeepers were not designated with respect to all the core platform services they notified; indeed, some of them filed a submission rebutting the quantitative criteria. The Commission approached the rebuttal proposals in two ways: in some cases, it accepted the rebuttals immediately, without the market investigation foreseen by the

8 The list of notified transactions is accessible at https://digital-markets-act-cases.ec.europa.eu/acquisitions.

9 The list of gatekeepers is accessible at https://digital-markets-act.ec.europa.eu/gatekeepers_en.

10 Meta's and Apple's cases are registered by the General Court as *Meta Platforms v. Commission* T-1078/23 and *Apple v. Commission* T-1080/23. The ByteDance judgment is Judgment of the General Court of 17 July 2024 on the case *ByteDance v. Commission*, T-1077/23; the appeal case is registered by the CJEU as C-627/24 P.

DMA. This was the case of Samsung, who only notified Samsung's Internet Browser and thus was not designated as a gatekeeper at all. Alphabet and Amazon are gatekeepers in relation to their other core platform services but were not designated with respect to Alphabet's Gmail and Microsoft's Outlook.com (European Commission, 6 September 2023). Such a procedure is not explicitly supported by the text of the DMA (Martínez, 2024a, p. 286); the Commission was however satisfied that the rebuttals not only 'manifestly called into question' the presumptions, as required by the DMA, but also 'clearly demonstrated that the services do not constitute an important gateway' for business users to reach end users (European Commission, 5 September 2023, Alphabet).

In parallel, as a second and, from the text of the DMA's point of view, 'standard' procedure to rebut the quantitative presumptions, the Commission opened four market investigations, concerning Apple's iMessage and Microsoft's Bing, Edge and Microsoft Advertising. The Commission ultimately decided that these do not qualify as gatekeeper services (European Commission, 13 February 2024). Conversely, the Commission opened an investigation concerning Apple's iPadOS and ultimately designated it on the basis of qualitative criteria, as the quantitative thresholds were not met (European Commission, April 2024). Finally, the Commission received a new wave of notifications on 1 March 2024 (European Commission, 1 March 2024). The Commission designated Booking.com on 13 May 2024 (European Commission, May 2024). Conversely, it decided immediately not to designate X's X Ads and ByteDance's TikTok Ads. After a market investigation, it decided on 16 October 2024 that X's online social networking service X does not qualify either (European Commission, October 2024).

Concerning the designation procedure, even though we are still waiting for the General Court's judgments on Apple and Meta and the CJEU's judgment on ByteDance, we may already formulate several observations concerning the practice hitherto. It has been claimed that 'the designation process did not strictly follow the letter of law', as the designations 'demonstrate a broad use of discretion on the European Commission's side' (Martínez, 2024a, p. 268). As a result, the designation process was not 'entirely consistent' in all the cases (Martínez, 2024a, p. 290). Indeed, the designation process is flexible (Bania & Geradin, 2025, p. 109), and the General Court leaves the Commission with a wide margin of discretion (Martínez, 2024b, p. 539). At the same time, the DMA's purpose was specifically to allow for a fast designation, unlike the cumbersome process of establishing dominant position. The DMA seems to be successful in this regard, while the Commission still manages to thoroughly review the arguments of the parties (Bania & Geradin, 2025, p. 126). In the text below, we will concentrate on two features that stand out in practice so far.

3.1. The characteristics of core platform services

Two issues concerning the notion of core platform services that have been discussed in the case law to date merit attention. The first is the business-to-consumer characteristic of core platform services; the second is the 'delineation' of individual

services. Concerning the former, an undertaking may be designated a gatekeeper if it provides a core platform service which is an important gateway for businesses to reach consumers (DMA, Art. 3(1)(b)). The designation decisions issued so far 'demonstrate that this element is key to performing gatekeeper designation' (Martínez, 2025, p. 2). It was the crucial element of the first and only designation, based on qualitative criteria, of iPadOS (Martínez, 2025, p. 3). Thus Apple's iMessage was not designated, as the Commission found out in a market investigation that iMessage should not be listed as an important gateway for business users to reach end users (European Commission, 12 February 2024, para. 38). More attention was dedicated to Meta's Facebook Marketplace. Meta claimed that it is now a purely consumer-to-consumer service, which the Commission denied (European Commission, 5 September 2023, Meta, para. 256). The Commission first stressed that it needs to take into account the last three financial years; Meta introduced its changes to Facebook Marketplace only in 2023. More importantly, the Commission suggested that the data provided by Meta show that a majority of the Marketplace's users actually act in a professional or commercial capacity (European Commission, 5 September 2023, Meta, para. 258). According to the Commission, the fact that Meta does not explicitly 'allow' business users to use the Marketplace in order to reach consumers is irrelevant, as their practice suggests they still do so (European Commission, 5 September 2023, Meta, para. 266). These arguments are still pending before the General Court.

Similar arguments were raised by ByteDance with respect to TikTok and were dismissed by the Commission. In addition, the Commission criticised ByteDance's methodology for identifying business users (Bania & Geradin, 2025, p. 120). Without going into technical details on this issue, I will discuss ByteDance's arguments in more detail in the section below, in connection with the General Court's judgment on its action for annulment.

The second issue that ought to be discussed is the process of 'delineation', not foreseen by the DMA (Martínez, 2024a). As a 'preliminary step', the Commission starts with 'delineation of services', i.e. distinguishing individual core platform services provided by the potential gatekeeper and defining their boundaries (European Commission, 5 September 2023, Alphabet, para. 15). It is not a market definition as known in competition law; indeed, the delineation of core platform services has no bearing on the definition of the relevant market for the purpose of applying EU competition rules (and vice versa), and those two types of analyses may thus lead to different results (European Commission, 5 September 2023, Alphabet, para. 19). Gatekeepers are obliged to 'delineate' their services in their notification, and they even have to suggest possible alternative delineations (European Commission, 2023, Annex I, Section 2.1).

The DMA lists ten categories of core platform services (DMA, Art. 2(2)). According to the Commission, the core platform services may be considered distinct even if they fall within the same category; in such cases, a relevant criterion for iden-

tifying distinct services within the same category is the purpose for which it is used by either end users or business users, or both. Different services may constitute a single core platform service if they are used for the same purpose by both an end user and a business, unless they fall within different categories (European Commission, 5 September 2023, Alphabet, para. 17). Though clear in the abstract, such delineation gets very complex in specific cases. Unfortunately, the Commission has used a different depth of argumentation in different cases, based on its dialogue with the gatekeepers concerned (Martínez, 2024a, p. 271). At the same time, even though the purpose of the services should have been the key factor in delineating them (e.g. European Commission, 5 September 2023, Alphabet, para. 16), the Commission sometimes relies on other criteria (Martínez, 2025, p. 3).

Interestingly, in some seemingly identical cases the Commission arrives at different conclusions. Hardware technology may be used as an example. Google's Android is regarded as a single core platform service, whereas in the case of Apple, iOS and iPadOS are differentiated. The difference lies in the fact that whereas Apple produces both the hardware and the software which is designed specifically for the individual hardware's purposes, the Android operating system is used on a wide range of different products (European Commission, 12 February 2024, Apple, paras. 84–90; Martínez, 2024a, p. 276). Conversely, Microsoft's Windows PC operating system was designated as a single platform service, despite the differences in its design for x86 and x64 processors (European Commission, 5 September 2023, Microsoft, paras. 30–31; Martínez, 2024a, p. 276). Similarly, the AppStore was designated a single intermediation service across the different iOS systems (European Commission, 12 February 2024, Apple, para. 39). This is contested in Apple's action for annulment (Bania & Geradin, 2025, p. 122), but the General Court has not yet decided.

The second question concerning delineation is the qualification of individual core platform services. For example, Meta's Facebook is a 'social network' and Messenger a 'number-independent interpersonal communications service', and these two thus constitute distinct core services, even though Messenger was originally only a chat functionality of Facebook (European Commission, 5 September 2023, Meta, para. 177). This finding is challenged by the action for annulment (Bania & Geradin, 2025, p. 123); the General Court has, however, not yet decided. Conversely, both Meta's Facebook and Instagram were delineated as 'social networks'. Even though Meta argued that Facebook and Instagram constitute the same core platform service, the Commission decided they are different (European Commission, 5 September 2023, Meta, para. 44), based predominantly on the lack of integration of these services, not their distinctive purpose (Martínez, 2025, p. 3). The delineation may sometimes be controversial. For example, ByteDance's TikTok was qualified as a 'social network', not a 'video-sharing platform', as it argued (European Commission, 5 September 2023, ByteDance, para. 66). The General Court confirmed the Commission's arguments.

3.2. Rebutting the quantitative presumption

Undertakings have a limited space to rebut a presumption based on the quantitative criteria, contained in Article 3(2) of the DMA. The required legal standard is very high (Martínez, 2024a, p. 286), and successful rebuttal is presented as an exception (Schmidt & Hübener, 2023, p. 31). The submission is physically limited to 30 pages (European Commission, 2023, Annex II). Most interesting, however, is the limitation of arguments that can be raised. When the Commission designates an undertaking not meeting the quantitative criteria, it builds its decision on a number of qualitative arguments, outlined in Article 3(8) of the DMA. One would expect that similar arguments would be used in reverse order, i.e. to rebut the quantitative presumption. Rather surprisingly, and in contradiction to the Commission's original proposal, the DMA only allows quantitative criteria during the rebuttal procedure (Bania & Geradin, 2025, p. 102). According to Recital 23 of the DMA, 'the Commission should take into account only those elements which directly relate to the quantitative criteria'. This has been criticised by some commentators (Bania & Geradin, 2025, p. 105).

Interestingly, all the rebuttal submissions have contained not only quantitative but also qualitative arguments (Martínez, 2024a, p. 284), and even more importantly, the Commission took them into account (Bania & Geradin, 2025, p. 112), sometimes even giving more weight to them than to the quantitative ones (Bania & Geradin, 2025, p. 114). For example, with regard to Microsoft's Outlook.com, the Commission took into account the (quantitative) very high number of users of this service, but balanced it against the (qualitative) absence of lock-in effects and switching restrictions (European Commission, 5 September 2023, Microsoft, para. 130).

The General Court more or less closed this dispute in its recent ByteDance judgment. It decided that the separation of 'qualitative' and 'quantitative' arguments is merely 'artificial' (Judgment of the General Court of the European Union, 2024, para. 40). The General Court therefore concluded that the undertakings concerned may 'submit, in order to rebut the presumptions laid down in Article 3(2) of the DMA, arguments and evidence, whether or not they are expressed in figures, provided that they relate directly to one or more of those presumptions' (Judgment of the General Court of the European Union, 2024, para. 51). On the merits, however, this did not help ByteDance to win its case against the designation of TikTok.[11] The General Court also recalled that the designation process is based on a 'specific regulatory framework' aimed at enabling fast decision-making. Therefore the rebuttal arguments must be contained in the notification submission and cannot be raised later, not even in front of the court (Judgment of the General Court of the European Union, 2024, para. 233).

11 For detailed discussion of the judgment, see e.g. Martínez, 2024b.

4. Compliance with the DMA

What has the DMA achieved so far? One company that was supposed to benefit from it described it as an 'utter failure' (John, 2025). Some rules for the core platform services have changed, but do they 'fully and effectively' comply with the DMA?

4.1. Regulatory dialogue

Rather surprisingly, the 'regulatory dialogue' procedure has not yet been initiated upon a gatekeeper's request (DMA, Art. 8(3)). Conversely, the Commission has opened two proceedings with Apple in September 2024, on the basis of Article 8(2) DMA, in relation to Apple's interoperability obligations (European Commission, September 2024). The first concerns the iOS connectivity features for other digital devices, the second the procedure for developers interested in obtaining interoperability with iPhone and iPad features.

In December 2024, the Commission made its 'Overview of proposed measures' public and opened a public consultation, asking third parties to comment on the proposal (European Commission, December 2024). In March 2025, it adopted two detailed decisions specifying the interoperability obligations (European Commission, 2025a), which Apple will have to comply with. Overall, the whole procedure seems more like a 'regulatory imposition' of obligations than a 'regulatory dialogue' (Martínez, 2025, p. 9). From all the information made public, it seems that the Commission's role was decisive in framing the specific obligations Apple needs to comply with. This was already evident from the 'Overview of proposed measures' of December 2024, which is in fact a very detailed list of technological features meriting regulatory transformation. The fact that the procedure is in fact significantly more unilateral than the name 'dialogue' would suggest is already obvious from the introductory phrases the Commission employs: the Commission 'is assisting Apple in its compliance by detailing the measures needed for enabling interoperability with iOS for third-party connected devices and by streamlining the process put in place by Apple to handle future requests for interoperability with iPhone and iPad devices' (European Commission, 2025a).

It remains to be seen how the Commission's practice will develop in the future. As mentioned earlier, the platforms may be reluctant to change their practices; a proper dialogue might therefore be insufficient to make them do so. Indeed, business users and other stakeholders have expressed 'concerns about the lack of effective engagement of the designated DMA gatekeepers' (European Businesses, 2024). At the same time, the idea of obligations determined in concert by the regulator and the regulated is one of the methodological cornerstones of the DMA. The Commission is an extraordinarily experienced enforcer; under the DMA, it will need to learn to be more attentive to what the platforms have to say.

4.2. Non-compliance proceedings

For the core platform services designated in the first wave of decisions in September 2023, the deadline for compliance was March 2024. All the gatekeepers submitted their compliance reports on time. The published versions varied greatly in detail, with, on the one side, very detailed reports provided by Alphabet, ByteDance and Meta, and on the other, very brief ones provided by Amazon and Apple (Martínez, 2025, p. 6). The Commission was reportedly 'not super happy' with the lack of detail in some reports and confirmed that third parties are 'very justified' in demanding that the reports provide more meaningful details explaining compliance measures (Baxter, 2024).

Two weeks later, the Commission formally opened four non-compliance investigations in accordance with Article 29 DMA for possible breach of several DMA obligations, in conjunction with a possible breach of the 'anti-circumvention' Article 13 DMA. The first putatively breached obligation is Article 5(2) DMA. The Commission has opened proceedings against Meta to investigate whether the recently introduced 'pay or consent' model for users in the EU complies with Article 5(2), which requires gatekeepers to obtain consent from users when they intend to combine or cross-use their personal data across different core platform services. The Commission is concerned that the binary choice imposed by Meta's 'pay or consent' model may not provide a real alternative if users do not consent, thereby not achieving the objective of preventing the accumulation of personal data by gatekeepers (European Commission, 25 March 2024). In July 2024, the Commission informed Meta of its preliminary findings that its 'pay or consent' advertising model fails to comply with the DMA (European Commission, July 2024).

The second is the obligation under Article 5(4) DMA. The Commission has opened proceedings to assess whether the measures implemented by Alphabet and Apple in relation to their obligations pertaining to app stores are in breach of the DMA. Article 5(4) requires gatekeepers to allow app developers to 'steer' consumers to offers outside the gatekeepers' app stores, free of charge. The Commission is concerned that Alphabet's and Apple's measures may not be fully compliant, as they impose various restrictions and limitations. These constrain, among other things, developers' ability to freely communicate and promote offers and directly conclude contracts, including by imposing various charges (European Commission, 25 March 2024). In June 2024, the Commission informed Apple about its preliminary findings on a breach of this provision (European Commission, June 2024). Alphabet was addressed with preliminary findings of non-compliance in March 2025 (European Commission, 2025b).

Third, an obligation under Article 6(3) DMA might have been breached. The Commission has opened proceedings against Apple regarding its measures to comply with obligations to (1) enable end users to easily uninstall any software applications on iOS, (2) enable end users to easily change default settings on iOS, and (3)

prompt users with choice screens which must effectively and easily allow them to select an alternative default service, such as a browser or search engine, on their iPhones. The Commission is concerned that Apple's measures, including the design of the web browser choice screen, may be preventing users from truly exercising their choice of services within the Apple ecosystem, in contravention of Article 6(3) (European Commission, 25 March 2024).

Fourth, the Commission's concerns also focus on Article 6(5) DMA. It has opened proceedings against Alphabet to determine whether its display of Google search results may lead to self-preferencing in relation to Google's vertical search services (e.g. Google Shopping, Google Flights, Google Hotels) over similar rival services. The Commission is concerned that the measures Alphabet implemented to comply with the DMA may not ensure that third-party services featuring on Google's search results pages are treated in a fair and non-discriminatory manner, in comparison to Alphabet's own services, as required by Article 6(5) DMA (European Commission, 25 March 2024). A preliminary finding of non-compliance was published in March 2025 (European Commission, 2025b). The Commission is also gathering evidence in connection with possible self-preferencing by Amazon (European Commission, 25 March 2024); however, a formal investigation has not yet been opened.

Finally, the Commission started to investigate Apple's new fee structure and other terms and conditions for alternative app stores and the distribution of apps from the web (sideloading) which may be defeating the purpose of its obligations under Article 6(4) DMA (European Commission, 25 March 2024). In this regard, a formal investigation was opened in June 2024 (European Commission, June 2024).

Notwithstanding the 12-month deadline for closing non-compliance procedures, and the fact that the Commission has published its preliminary non-compliance findings relatively quickly, no final decisions had been adopted by the end of March 2025.[12] The space to comment on the Commission's approach to securing compliance with the DMA is therefore limited. Several features of the Commission's approach may nonetheless be observed.

4.3. The Commission's approach so far

Four observations may be made concerning the Commission's practice hitherto. First, it is clearly willing to take advice from other market players affected by the gatekeepers' conduct (Ingemarsson & Bichet, 2024, p. 337). Even though it is not required by the DMA itself, the Commission has been organising workshops with stakehold-

12 By the date of publication of this article, these decisions have been issued: European Commission, 22 April 2025, Apple; European Commission, 23 April 2025, Apple; European Commission, 23 April 2025, Meta; European Commission, 12 November 2025, Alphabet

ers, discussing the compliance of individual gatekeepers.[13] Similarly, there were public consultations before adopting the regulatory dialogue decisions, as discussed in section 4.1 above.

Second, the Commission is not satisfied with only 'technical' compliance, proposed by the gatekeepers, but rather seeks a complete transformation of the platforms' models (Martínez, 2025, p. 7). This is confirmed by the fact that the anti-circumvention Article 13 DMA was employed in all the non-compliance cases. It has been claimed that 'significant resistance to full compliance with the DMA is to be expected' (Bania & Geradin, 2025, p. 237). The preliminary findings published by the Commission so far suggest that it is trying honestly to change the way in which markets operate in favour of more openness and interoperability.

Third, the procedure is significantly different from the investigations under Articles 101 and 102 TFEU. Even though there is a possibility of carrying out on-site inspections (DMA, Art. 23) in a way corresponding with Regulation 1/2003 (Council of the EU, 2002), this power has not yet been used in a case of non-compliance, thus confirming the dialogue-based nature of the DMA. Similarly, the deadline for issuing preliminary findings, an instrument akin to the statement of objections under Regulation 1/2003, is three months (DMA, Art. 8(5)); the Commission was actually able to issue its preliminary findings even earlier. Conversely, three times as long (nine months) is reserved for the rest of the proceedings. This contrasts with the proceedings under Regulation 1/2003, where the statement of objections tends to be issued by the end of the proceedings and the remaining part of the proceedings is relatively short. This again leaves a possibility for the Commission to enter into dialogue with the gatekeeper under the DMA.

Finally, all the regulatory efforts should ultimately benefit the final consumers; the effectiveness of the DMA therefore ultimately depends on the behaviour of end users (Bania & Geradin, 2025, p. 234). If consumers do not actually exploit the possibilities opened by the new regulation, the DMA could be regarded as a failure. The compliance requirements therefore need to be devised in a way rooted in behavioural economics; it should be the gatekeepers' duty to show that they have taken the findings of this science into account (Fletcher & Vasas, 2024, p. 462).

Conclusions

The aim of this paper was to evaluate the practice to date concerning the application of the DMA. In conclusion, several trends can be identified. First, the Commission has clarified the concept of the gatekeeper and has developed a procedure for their designation, which, though stretching beyond the text of the DMA, seems to be

13 A dedicated webpage is accessible at https://digital-markets-act.ec.europa.eu/events/workshops_en.

effective. Most importantly, the Commission's interpretation was approved in the first proceedings before the General Court. Similarly, the notion of a core platform service and the rebuttal procedure have been clarified.

Second, the gatekeepers are clearly technically fulfilling all their obligations, but are nonetheless avoiding a significant transformation of their business models. Because of that, the Commission has had to open a number of non-compliance proceedings. The gatekeepers' lack of willingness to undergo significant transformation of their business models may also be derived from the fact that they have not initiated regulatory dialogues with the Commission; the specification procedure has been used only once. It seems to be the case that these businesses are only willing to make as few changes as possible.

Third, even though some positive changes in the digital markets may arguably already be observed (Ingemarsson & Bichet, 2024, p. 337), these changes affect only the EU markets. The 'Brussels effect', the hope that EU regulation would have a worldwide effect on the practices of global undertakings, has not materialised (Martínez, 2025, p. 7). This does not need to be viewed as the DMA's failure: the regulatory differences in different markets will work as a 'natural experiment', enabling the actual effects of the DMA in practice to be measured by future research.

REFERENCES

Akaman, P. (2022). Regulating competition in digital platform markets: A critical assessment of the framework and approach of the EU Digital Markets Act. *European Law Review*, *47*(1), 85–109.

Bania, K., & Geradin, D. (Eds.). (2025). *The Digital Markets Act: A guide to the regulation of big tech in the EU*. Hart Publishing.

Baxter, R. (2024). *European Commission sets sights on DMA compliance reports*. Global Competition Review. https://globalcompetitionreview.com/article/european-commission-sets-sights-dma-compliance-reports

Botta, M. (2021). Sector regulation of digital platforms in Europe: Uno, nessuno e centomila. *Journal of European Competition Law & Practice*, *12*(7), 500–512.

Cohen, J. E. (2018). Law for the platform economy. *Georgetown Law Technology Review*, *2*(2), 191–196.

European Businesses. (2024) Public statement of European companies and industry groups. https://eutechalliance.eu/wp-content/uploads/2024/01/Public-statement-calling-on-Gatekeepers-to-cooperate-16-Jan-2024pdf.pdf

European Commission. (2020a). Proposal for a Regulation of the European Parliament and of the Council on Contestable and Fair Markets in the Digital Sector (Digital Markets Act), COM/2020/842 final.

European Commission. (2020b). *Impact assessment of the Digital Markets Act*. https://digital-strategy.ec.europa.eu/en/library/impact-assessment-digital-markets-act

European Commission. (2023). Commission Implementing Regulation (EU) 2023/814 of 14 April 2023 on Detailed Arrangements for the Conduct of Certain Proceedings by the Commission Pursuant to Regulation (EU) 2022/1925 of the European Parliament and of the Council.

European Commission. (2023, 4 July). *Potential gatekeepers notified the Commission and provided relevant information*. https://digital-markets-act.ec.europa.eu/potential-gatekeepers-notified-commission-and-provided-relevant-information-2023–07-04_en

European Commission. (2023, 5 September). Commission Decision of 5 September 2023, case DMA.10002 et al. *Alphabet*. https://digital-markets-act-cases.ec.europa.eu/cases/DMA.100002

European Commission. (2023, 5 September). Commission Decision of 5 September 2023, case DMA.100040 *ByteDance – Online social networking services*. https://digital-markets-act-cases.ec.europa.eu/cases/DMA.100040

European Commission. (2023, 5 September). Commission Decision of 5 September 2023, case DMA.10020 et al. *Meta*. https://digital-markets-act-cases.ec.europa.eu/cases/DMA.100020

European Commission. (2023, 5 September). Commission decision of 5 September 2023, case DMA.100017 et al. *Microsoft* https://digital-markets-act-cases.ec.europa.eu/cases/DMA.100017

European Commission. (2023, 6 September). *Commission designates six gatekeepers under the Digital Markets Act*. https://digital-markets-act.ec.europa.eu/commission-designates-six-gatekeepers-under-digital-markets-act-2023–09-06_en

European Commission. (2024). Report from the Commission to the Council and the European Parliament: Annual Report on Regulation (EU) 2022/1925 of the European Parliament and of the Council on Contestable and Fair Markets in the Digital Sector and Amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act), COM(2024) 106 final. https://digital-markets-act.ec.europa.eu/about-dma/dma-annual-reports_en

European Commission. (2024, 12 February). Commission Decision of 12 February 2024, case DMA.10022 *Apple – number-independent interpersonal communications services*. https://digital-markets-act-cases.ec.europa.eu/cases/DMA.100022

European Commission. (2024, 13 February). *Commission closes market investigations on Microsoft's and Apple's services under the Digital Markets Act*. https://digital-markets-act.ec.europa.eu/commission-closes-market-investigations-microsofts-and-apples-services-under-digital-markets-act-2024–02-13_en

European Commission. (2024, 1 March). *Booking, ByteDance and X notify their potential gatekeeper status to the Commission under the Digital Markets Act*. https://digital-markets-act.ec.europa.eu/booking-bytedance-and-x-notify-their-potential-gatekeeper-status-commission-under-digital-markets-2024–03-01_en

European Commission. (2024, 25 March). *Commission opens non-compliance investigations against Alphabet, Apple and Meta under the Digital Markets Act*. https://ec.europa.eu/commission/presscorner/detail/en/ip_24_1689

European Commission. (2024, 29 April). *Commission designates Apple's iPadOS under the Digital Markets Act*. https://digital-markets-act.ec.europa.eu/commission-designates-apples-ipados-under-digital-markets-act-2024–04-29_en

European Commission. (2024, 13 May). *Commission designates Booking as a gatekeeper and opens a market investigation into X*. https://digital-markets-act.ec.europa.eu/commission-designates-booking-gatekeeper-and-opens-market-investigation-x-2024–05-13_en

European Commission. (2024, 24 June). *Commission sends preliminary findings to Apple and opens additional non-compliance investigation against Apple*. https://digital-markets-act.ec.europa.eu/commission-sends-preliminary-findings-apple-and-opens-additional-non-compliance-investigation-2024–06-24_en

European Commission. (2024, 1 July). *Commission sends preliminary findings to Meta over its 'pay or consent' model for breach of the Digital Markets Act*. https://digital-markets-act.ec.europa.eu/commission-sends-preliminary-findings-meta-over-its-pay-or-consent-model-breach-digital-markets-act-2024–07-01_en

European Commission. (2024, 19 September). *Commission starts first proceedings to specify Apple's interoperability obligations under the Digital Markets Act*. https://ec.europa.eu/commission/presscorner/detail/en/ip_24_4761

European Commission. (2024, 16 October). *Commission concludes that online social networking service of X should not be designated under the Digital Markets Act*. https://digital-markets-act.ec.europa.eu/commission-concludes-online-social-networking-service-x-should-not-be-designated-under-digital-2024–10-16_en

European Commission. (2024, 18 December). *DMA.100203 – Consultation on the proposed measures for interoperability between Apple's iOS operating system and connected devices*. https://digital-markets-act.ec.europa.eu/dma100203-consultation-proposed-measures-interoperability-between-apples-ios-operating-system-and_en

European Commission. (2025a, 19 March). *Commission provides guidance under Digital Markets Act to facilitate development of innovative products on Apple's platforms*. https://ec.europa.eu/commission/presscorner/detail/en/ip_25_816

European Commission. (2025b, 19 March). *Commission sends preliminary findings to Alphabet under the Digital Markets Act*. https://ec.europa.eu/commission/presscorner/detail/en/ip_25_811

European Commission. (2025, 22 April). Commission Decision of 22 April 2025, case DMA.100109 *Apple – Online Intermediation Services – app stores – AppStore – Art. 5(4)*. https://digital-markets-act-cases.ec.europa.eu/cases/DMA.100109

European Commission. (2025, 23 April). Commission Decision of 23 April 2025, case DMA.100185 *Apple – Operating systems – iOS – Art. 6(3)*. https://digital-markets-act-cases.ec.europa.eu/cases/DMA.100185

European Commission. (2025, 23 April). Commission Decision of 23 April 2025, case DMA.100055 *Meta – Article 5(2)*. https://digital-markets-act-cases.ec.europa.eu/cases/DMA.100055

European Commission. (2025, 12 November). Commission Decision of 12 November 2025, case DMA.100231 *Alphabet – Google Search – Site reputation abuse policy*. https://digital-markets-act-cases.ec.europa.eu/cases/DMA.1000231

Council of the EU. (2002). Council Regulation (EC) no. 1/2003 of 16 December 2002 on the Implementation of the Rules on Competition Laid Down in Articles 81 and 82 of the Treaty. OJ L 1, 4.1.2003, pp. 1–25

Council of the EU. (2004). Council Regulation (EC) no. 139/2004 of 20 January 2004 on the Control of Concentrations between Undertakings (the EC Merger Regulation). OJ L 24, 29.1.2004, pp. 1–22

European Parliament and the Council of the EU. (2016). Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Re-

gard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation). OJ L 119, 4.5.2016, pp. 1–88

European Parliament and the Council of the EU. (2022a). Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on Contestable and Fair Markets in the Digital Sector and Amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act). OJ L 265, 12.10.2022

European Parliament and the Council of the EU. (2022b). Regulation (EU) 2022/2065 of the European Parliament and the Council of 19 October 2022 on a Single Market for Digital Services and Amending Directive 2000/31/EC (Digital Services Act). OJ L 277, 27.10.2022, pp. 1–102

European Parliament and Council of the EU. (2022c). Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European Data Governance and Amending Regulation (EU) 2018/1724 (Data Governance Act). OJ L 152, 3.6.2022, pp. 1–44

European Parliament and Council of the EU. (2023). Regulation (EU) 2023/2854 of the European Parliament and of the Council of 13 December 2023 on Harmonised Rules on Fair Access to and Use of Data and Amending Regulation (EU) 2017/2394 and Directive (EU) 2020/1828 (Data Act). OJ L, 2023/2854, 22.12.2023, pp. 1–71

Evans, D. S. (2003). The antitrust economics of multisided platform markets. *Yale Journal on Regulation*, *20*(2), 325–381.

Fletcher, A., & Vasas, Z. (2024). Implementing the DMA: The role of behavioural insights. *Journal of European Competition Law & Practice*, *15*(7), 456–462.

Gönenç, G., Kağan, A., & Yildiz, G. (2022). Is there a need for a visible hand in digital markets? *European Competition and Regulatory Law Journal*, *6*(4), 306–317.

Ibáñez-Colomo, P. (2021). The draft Digital Markets Act: A legal and institutional analysis. *Journal of European Competition Law & Practice*, *12*(7), 561–575.

Ingemarsson, R., & Bichet, P. (2024). Survey on the Digital Markets Act and digital policy: A year into the application of one of the most innovative regulatory tools (2023–2024). *Journal of European Competition Law & Practice*, *15*(5), 330–338.

Jenny, F. (2021). Changing the way we think: Competition, platforms and ecosystems. *Journal of Antitrust Enforcement*, *9*(1), 1–18.

John, B. (2025, 18 February). *DMA branded an 'utter failure' as first anniversary nears*. Global Competition Review. https://globalcompetitionreview.com/article/dma-branded-utter-failure-first-anniversary-nears

Judgment of the General Court of the European Union of 17 July 2024 on the case *ByteDance v. Commission*, T-1077/23.

Martínez, R. A. (2024a). The requisite legal standard of the Digital Market Act's designation process. *Journal of Competition Law & Economics*, *20*(4), 265–291.

Martínez, R. A. (2024b). Rebutting gatekeeper presumptions in the Digital Markets Act: Case T-1077/23 ByteDance Ltd v European Commission. *Journal of European Competition Law & Practice*, *15*(8), 537–539.

Martínez, R. A. (2025). Survey on the Digital Markets Act: 2024, compliance starts. *Journal of European Competition Law & Practice*, *16*(6), 390–398.

Monti, G. (2021). The Digital Markets Act: Improving the institutional design. *Journal of European Competition Law & Practice*, *12*(2), 90–101.

Montjoye, Y.-A., Schweitzer, H., & Crémer, J. (2019). *Competition policy for the digital era*. EU Publications Office.

Morbel, M. C. (2023). Regulating digital gatekeepers: The Digital Markets Act. *European Competition and Regulatory Law Review*, *8*(4), 206–215.

Newman, J. M. (2021, 29 January). *Antitrust in attention markets: Definition, power, harm* [Legal Studies Research Paper no. 3744839]. University of Miami. https://ssrn.com/abstract=3745839

Organisation for Economic Co-operation and Development (OECD). (2021). *Ex ante regulation of digital markets: OECD Competition Committee discussion paper*. OECD Publishing.

Organisation for Economic Co-operation and Development (OECD). (2022). *OECD handbook on competition policy in the digital age*. OECD Publishing.

Petr, M. (2024). Digital Markets Act and competition law: Is there an issue of ne bis in idem? *Yearbook of Antitrust and Regulatory Studies*, *17*(30), 155–170.

Schmidt, J. P., & Hübener, F. (Eds.). (2023). *New Digital Markets Act: A practitioners' guide*. Nomos Verlagsgesellschaft.

Solek, L. (2021). Need to revise or apply the concept of market definition with a view to 'zero-price' and overarching markets. *Journal of European Competition Law & Practice*, *12*(8), 593–603.

Tyagi, K., Sanders, A. K., & Cauffman, A. (Eds.). (2024). *Digital platforms, competition law, and regulation*. Hart Publishing.

Vesterdorf, B., & Fountoukalos, K. (2021). A new competition tool into old bottles? Considerations on the legal design of the European Commission's proposed NCT 2021. *Journal of European Competition Law & Practice*, *12*(4), 284–300.

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

sciendo

DOI: 10.15290/bsp.2026.31.01.10

Received: 21.06.2025
Accepted: 10.01.2026

Aleksandrs Potaičuks
Riga Graduate School of Law, Latvia
aleksandrs.potaicuks@rgsl.edu.lv
ORCID ID: 0009–0009–8795–2867

Commercial Registers as Administrative Databases: Balancing Public Accessibility and Privacy

Abstract: Countries develop various administrative databases in order to better perform governmental functions or to specifically influence certain civil relations or the behaviour of individuals. One particular and distinctive type of database containing personal data is commercial registers in Europe, which have a specific characteristic: they are accessible to the public and the data published has a binding nature. At the same time, this public accessibility of the personal data in commercial registers, especially with the increasing availability of digital technologies and their impact on society, can create a conflict with the privacy of the individuals included in these databases. This article first examines commercial registers as a form of public digitalisation, and then how the European Court of Justice, in its case law, balances the public accessibility which is an integral part of commercial registers with the right to privacy and data protection. In conclusion, the article generalises the lessons from the European Court of Justice case law and from legal scholarship that can be applied to preserve privacy, while the public accessibility of commercial registers is respected.

Keywords: databases, GDPR, privacy, proportionality of state measures, ReNEUAL model rules

Introduction

Countries develop various administrative databases (Lisičar & Jurić, 2024, p. 14) in order to better perform governmental functions or to specifically influence certain civil relations or the behaviour of individuals. In this regard, administrative databases and digitalisation are becoming increasingly important in the field of administrative law (Motzfeldt & Næsborg-Andersen, 2018, p. 138). In fact, the new ReNEUAL model rules on EU administrative procedure already include special provisions on

administrative databases, thus marking a new dimension for administrative law (Hofmann et al., 2014, p. 250).

One particular and distinctive type of database containing personal data is commercial registers in Europe, which, compared to other databases such as electronic health record systems or population registers, have a specific characteristic – they are publicly accessible and the data disclosed in them is binding. At the same time, this online availability of personal data and the public accessibility of commercial registers, especially with the increasing availability of digital technologies and their impact on society (Costa, 2023; Jabłoński, 2025, p. 162; Mazur & Ramiro Troitiño, 2024; Papacharissi & Gibson, 2011, p. 84), can create a conflict with the privacy of the individuals included in these databases. How can an individual claim their privacy given the public accessibility of commercial registers, and how can the balance of both be maintained?

The European Court of Justice (CJEU) has recently adopted at least four landmark judgments within a short period of time that balance data protection rights with the public accessibility that provides legal certainty in commercial registers; two more cases are still pending at the time of writing this article. As seen in one of the pending cases, the Constitutional Court of Latvia has also joined the debate, submitting another reference for a preliminary ruling on the protection of privacy in commercial registers (*Jautiva*, C-798/24).

This article employs a doctrinal research method centred on the analysis of CJEU case law relating to commercial registers in the European Union. While the research aim is to analyse the role of commercial registers and the principles established by the CJEU in its latest case law, the article raises a broader research question: how can transparency in commercial registers be balanced with privacy and data protection under European Union law in order to safeguard the fundamental rights of individuals? Thus, from a methodological point of view, this article focuses on the developments in CJEU case law and appraises the factors that controllers of commercial registers should take into consideration to avoid jeopardising fundamental rights, especially privacy and data protection.

While not denying the importance of public accessibility for commercial registers, in this paper I will examine commercial registers, as a form of public digitalisation, as well as existing CJEU case law to identify current data protection challenges and how the CJEU is shaping the GDPR. Firstly, in view of privacy concerns, I will analyse the special role of the commercial registers and the need for public accessibility. Secondly, I will present the leading cases concerning the intersection of privacy and commercial registers. Thirdly, I will generalise the lessons from the CJEU and demonstrate how the public accessibility of commercial registers is balanced with privacy in the age of public digitalisation and AI.

1. Commercial registers as administrative databases and their special role

Historically, commercial registers have evolved from the simple obligation to register a company and publish it in an official journal. Thus while historically, commercial registers used to be special books kept by commercial courts (Škorić, 2020, p. 3), today they are technologically advanced online databases containing a wealth of information for traders. Moreover, many public registers were in fact established and functioning long before data protection laws began to emerge (Lisičar & Jurić, 2024, p. 13).

In European countries, commercial registers are various (Heidemann, 2019, p. 19) and are operated and managed by very different public authorities: for example, in France and Germany there are authorised courts involved, whereas in Sweden, Denmark and Latvia there are agencies of a ministry. Today, however, the European Union has developed directives harmonising the rules for the creation and operation of a central register, commercial register or company register (hereinafter referred to as 'commercial registers') in the Member States (European Parliament & Council, 2017). Given the different nature of commercial registers, the focus of this research and the framework for the analysis of commercial registers as administrative databases is Directive (EU) 2017/1132 on certain aspects of company law.

Unlike many other administrative databases, such as population registers, electronic health record systems or criminal and law enforcement databases, commercial registers differ in specific features: firstly, information, including data on individuals, is not only stored for administrative purposes, but is also made available to the public; secondly, the information is not only publicly available, but also has a binding nature – it may be relied on by the company against third parties and thus provide legal certainty. Specifically, the purpose of disclosure of information in a commercial register is to protect the interests of third parties in relation to joint-stock and limited liability companies (Judgment of the CJEU, 2017), especially in situations where it is important to clarify who is authorised to bind the company (Judgment of the CJEU, 2024) or to assess good faith (Blajer, 2023, p. 114). The purpose of such disclosure is to enable any third person to inform themselves of these matters without having to establish a right or an interest to be protected (Judgment of the CJEU, 2017). Moreover, commercial registers differ from other types of administrative databases in that they are established in each Member State (de la Guardia, 2005). They therefore have a special role to play in improving trade between Member States and in creating the single market of the European Union (Judgments of the CJEU, 2017, 2024), especially as a form of digitisation (Ayata, 2024; Ferretti, 2022; Troitiño et al., 2024) or even the digital single market (Troitiño, 2022, p. 75). Registries and archives can also be seen as tools for developing the welfare state (Reichel & Chamberlain, 2021, p. 42).

The general standard for commercial registers as databases is that data may only be entered into a database for the legitimate purposes specified in the basic act (Hof-

mann et al., 2014, p. 250). Therefore the list of documents and particulars that must be disclosed by companies, kept by commercial registers and subsequently made available to the public is laid down by law (European Parliament & Council, 2017). This includes, for example, the instrument of constitution and statutes, the appointment, termination of office and particulars of the persons who are authorised to represent or take part in the administration, supervision or control of the company, the appointment of liquidators and particulars concerning them, etc. Currently in the European Union, in terms of the information to be disclosed to public, there is a dual approach: the EU legislation sets out the minimum information to be disclosed in order to harmonise the approach between Member States, while Member States' legislation may require more extensive disclosure of documents and particulars in their national laws (Judgment of the CJEU, 2024). This may also be relevant later when considering 'who is to blame' and the compatibility of the disclosure of personal data with the fundamental right to the protection of personal data and privacy, as some of these elements of information may or may not be considered personal data within the meaning of Article 4(1) of the GDPR (see section 2.1. on the notions of 'personal data' and 'processing' in the commercial register).

The information mentioned above, which is subject to compulsory disclosure in a commercial register and as such is made available to other businesses, is covered by public credibility (Gonet & Wolska, 2019, p. 86). Firstly, it is presumed that the data entered in public registers are true and consistent with actual and legal status (Gonet & Wolska, 2019, p. 86). Secondly, the commercial register's obligation to disclose information is closely related to the scope of information that is subject to statutory registration and storage by the commercial register (Judgment of the Supreme Court of Latvia, 2019). Thirdly, anyone who relies on publicly available register records which are subject to statutory disclosure must be presumed to be unaware of any existing inaccuracies contained in the records of the commercial register (Garnowski, 2022, p. 83). Thus the public credibility principle forms the cornerstone of commercial registers, and its most important effect is the promotion of legal certainty in commercial relations.

While the importance of such legal certainty is not contested, either historically or today, it is clearly evident that commercial registers have evolved from being special books kept by commercial courts into powerful digital databases, which puts much greater pressure on individuals' privacy. The increasing public accessibility, particularly influenced by technological advances such as search engines and artificial intelligence, forces us to look at public accessibility and privacy in a different light (Kerikmäe et al., 2019; Mokrá, 2023; Rek, 2024). Such reconsideration not only takes place in relation to databases; it also occurs more generally whenever any kind of information is published, including publicly available court judgments (Potaičuks & Tamužs, 2025, p. 5). It is important to bear in mind that the use of technology cannot happen at the expense of human rights or individual administrative rights. Therefore

it is important to strike a fair balance between, on the one hand, the specific objectives of the commercial register, and on the other, fundamental rights, especially privacy and data protection.

2. The scope of the right to private life covering entries in state administrative databases

2.1. The notions of 'personal data' and 'processing' in commercial registers

The next question is whether the fact that the data of private individuals related to a company are included (and processed) in a commercial register excludes these data from being classified as 'personal data' within the meaning of points 1 and 2 of Article 4 of the GDPR. There seems to be a misconception that all the data contained in a commercial register, including the persons who are authorised to represent the company or its liquidators, are considered to be data of the company, but are not 'personal data' as covered and protected by the GDPR. This seems to stem from Recital 14 of the GDPR, which states that 'this regulation does not cover the processing of personal data which concerns legal persons and in particular undertakings established as legal persons, including the name and the form of the legal person and the contact details of the legal person' (European Parliament & Council, 2016).

While it is true that the GDPR does not cover data that clearly relates to legal persons, including their name, form of registration and contact details (van der Sloot, 2015, p. 40), this cannot be overgeneralised in relation to all entries. The notions of 'personal data' and 'processing' were intentionally worded broadly and non-exhaustively in the GDPR and its preceding directive (Outeda, 2024; Purtova, 2018, p. 41). Data such as the name, contact details, etc., of natural persons representing a legal person are provided to a commercial register in the course of professional activity and normally fall within the wording of the definition of 'personal data' within the meaning of point 1 of Article 4 of the GDPR. Such an activity (provision of data to and storage in the commercial register, as well as disclosure) does not generally fall outside the scope of the GDPR, as defined in Article 2(2).

In this instance, the CJEU has ruled that 'the disclosure of the name, surname and contact details of natural persons representing a legal person falls within the meaning of point 1 of Article 4 of the GDPR' and 'this interpretation cannot be invalidated by recital 14 of the GDPR. The second sentence of that recital refers, inter alia, to the "name" and "contact details" of the legal person, and not that of the natural persons acting in the name of or on behalf of a legal person' (Judgment of the CJEU, 2025). Thus according to the CJEU, the disclosure of the data of natural individuals in this situation does indeed constitute the processing of 'personal data' (Judgments of the CJEU, 2017, 2024, 2025), and the fact that the disclosure is made for the purpose of the identification of the representation of the legal person is irrelevant (Judgment

of the CJEU, 2024). In this context, Article 161 of Directive 2017/1132 on company law and commercial registers also explicitly states that '[t]he processing of personal data carried out in the context of this Directive shall be subject to Directive 95/46/EC', and thus to the GDPR as well.

2.2. Direct and indirect disclosure of personal data in commercial registers

Disclosure of personal data in commercial registers can occur directly, when the personal data elements are the records themselves, or indirectly, when personal data is included in submitted documents and disclosed as part of a unit. Specifically, as seen in the case law, some particulars are 'disclosed directly', such as the names of persons who are authorised to represent or take part in the administration, and can be classified as personal data, whereas some particulars qualifying as personal data may be 'disclosed indirectly' (Judgment of the CJEU, 2024), such as the disclosure of the instrument of constitution or statutes (document) containing the names of the persons, their passport data or their signature (Judgment of the CJEU, 2024). In the latter situation, it is important to consider whether the personal data disclosed by the company can be qualified as subject to mandatory disclosure (and has a statutory basis requiring disclosure), complies with the data minimisation principle of the GDPR and is thus covered by the 'public credibility' principle.

3. Clashes between two competing interests: Public accessibility and the protection of privacy

Although commercial registers have been around for a while, the CJEU has in a short period of time received a number of preliminary rulings from Member States where public access to information has clashed with privacy and data protection. While case law shows that the rules on the protection of personal data do not prevent commercial registers from being subject to a fully open access regime (Lisičar & Jurić, 2024, p. 27), registers are still subject to specific measures that must be taken into account in order to balance data protection concerns. On its way from *Manni* to *Ministerstvo zdravotnictví*, the CJEU has provided significant clarification on the protection of personal data related to commercial registers and companies.

3.1. Manni (C-398/15): On the public availability of historical data in the commercial register

In *Manni*, the applicant objected to his personal data being accessible to the public in the commercial register 15 years after his former company had been declared insolvent and struck off the company register. The applicant alleged that the public availability of such historical data adversely affected his current business affairs, and requested the erasure of personal data relating to him in the commercial register. Thus this case showed the challenge of whether the former data protection directive

(now the GDPR) and the directive on the disclosure of company documents preclude a situation where any member of the public has access to data relating to natural persons contained in the commercial registers, without any time limit, and how public accessibility, the right to be forgotten and the principle of storage limitation are manifested in commercial registers (Judgment of the CJEU, 2017).

3.2. Luxembourg Business Registers (C-37/20): On the public accessibility of information on the beneficial ownership of companies

In *Luxembourg Business Registers*, due to anti-money laundering legislation, the applicant's data were made available in the commercial register to any member of the public, but the applicant wanted his personal data on the beneficial ownership to be restricted to a narrower public rather than available to anyone. The applicant argued that public access to his information could expose him and his family to 'a disproportionate risk of fraud, kidnapping, blackmail, extortion, violence and intimidation'. Thus this case raised the issue of the validity of the EU provision whereby information on the beneficial ownership of companies is made accessible in all cases to any member of the general public, incompatibly with the right to respect for private life and the protection of personal data as enshrined in the Charter of Fundamental Rights (the Charter) (Judgment of the CJEU, 2022).

3.3. Agentsia po vpisvaniyata (C-200/23): On the competence of a commercial register to erase personal data in the constitutive instrument of a company

In *Agentsia po vpisvaniyata*, after the founding of the company and the submission of the constitutive instrument to the commercial register, the personal data of the applicant contained in the constitutive instrument (including their surname, first name, ID number, ID card number, date and place of issue of that card, and the applicant's address and signature) were made available to the public through the register. The applicant requested the commercial register to erase the personal data from the publicly available constitutive instrument. However, the commercial register took the view that it is the applicant who must submit an authenticated copy of the constitutive instrument in which the personal data of the company members (other than the personal data required by law) were properly redacted, but the register itself was not able to edit personal data. Thus this case highlighted the challenge of whether national laws can prevent or restrict the erasure of personal data and how authorities maintaining commercial registers should comply with the 'right to erasure' procedures in commercial registers (Judgment of the CJEU, 2024).

3.4. Ministerstvo zdravotnictví (C-710/23): On whether the data relating to legal persons may be personal data

The dispute in *Ministerstvo zdravotnictví* concerns the individual's public access to official documents. A member of the public requested the Ministry of Health to provide information about a public purchase agreement, specifically the parties signing this agreement. Even though the Ministry provided the requested information, it redacted personal data from the issued documents, including the names, signatures, positions, and contact information of natural persons representing legal entities. Thus this case raised the question of whether information about natural persons representing legal entities constitutes personal data under the GDPR if it is used solely to identify legal entities (Judgment of the CJEU, 2025).

3.5. Pending cases: Jautiva (C-798/24) and Unione Fiduciaria (C-685/24)

In both *Jautiva* and *Unione Fiduciaria*, the national courts of Latvia and Italy referred the question to the CJEU to clarify whether the data required to be disclosed in the commercial registers to any member of the general public under national law – every shareholder of a joint-stock company in Latvia (*Jautiva*) and beneficial owners of trusts and similar legal arrangements in Italy (*Unione Fiduciaria*) – fall within the scope of information to be disclosed to the public in the light of existing European Union legislation on the protection of personal data. Neither case has yet been adjudicated.

4. Balancing public accessibility and privacy in the context of commercial registers

4.1. The scope of the right to private life and data protection covering entries in commercial registers

The analysis of the above-mentioned court cases shows that the disclosure of personal data (with online availability) in the commercial registers (which is required by law), in a way that makes the personal data available in all cases to any member of the general public, methodologically constitutes an interference with the fundamental rights enshrined in Articles 7 and 8 of the Charter. However, where such disclosure is ordered by national laws, it can constitute an interference under national constitutions as well and thus be deemed unconstitutional at a national level (Šulmane, 2025, p. 304).

Before registers were made accessible online, anyone wanting to receive data from a register would typically have had to visit the institution that controlled it and request the data in person (Lisičar & Jurić, 2024, p. 25). However, the online availability of data has changed people's habits and the extent to which privacy is impacted.

The CJEU in this regard has even considered that such online availability of, for example, beneficial ownership information constitutes 'a serious interference' (Judgment of the CJEU, 2022; Lisičar & Jurić, 2024, p. 24). This is due to the facts that (1) such information can be used to create a profile of the state of the person's wealth, investment choices, etc.; (2) online availability to a wide audience also gives access to people who, for reasons unrelated to the objective of the measure, may be able to find out about the material and financial situation of the data subject; and (3) similar to the Latin expression 'verbum semel emissum volat irrevocabile', once personal data are publicly disclosed by the register, it is extremely difficult to control successive processing, and thus the data subjects are unable to defend themselves against abuse (Judgment of the CJEU, 2022).

However, the fact that there is an interference with the fundamental right does not automatically lead to a violation of it, since, according to the case law and Article 52(1) of the Charter, Articles 7 and 8 of the Charter are not absolute and interference can be justified, considering these rights in relation to their function in the society (Judgment of the CJEU, 2022; Mudrecki, 2021, p. 41).

4.2. Balancing interests: A method of evaluating the justification for interference

For any limitation on the exercise of a fundamental right (including the right to privacy and data protection when personal data are disclosed to the public) to be considered justified, it must, firstly, be provided for by law; secondly, must respect the essence of those rights; thirdly, must meet objectives of general interest recognised by the EU; and fourthly, must be appropriate, necessary and proportionate. In the current case law, the strongest clashes between privacy and public accessibility in relation to commercial registers seem to occur mainly at the level of the third and fourth of these criteria. Consequently, the following sub-sections will first explain the most important conclusions of the judgments in relation to commercial registers, and will then provide a deeper analysis of the 'objectives of general interest' and 'appropriate, necessary and proportionate' criteria, which balance public accessibility and privacy.

4.3. Lessons for commercial registers: From Manni to Ministerstvo zdravotnictví

In *Manni* (on the right to be forgotten (Vardanyan et al., 2023, p. 97) in a commercial register after expiry of a sufficiently long period after the dissolution of a company), the CJEU was seemingly faced with a Gordian knot: the absence of heterogeneity in the limitation periods provided for in national laws and thus the impossibility of claiming that personal data are no longer necessary in a commercial register. While the CJEU acknowledged that storing personal data for longer than necessary could be problematic in terms of proportionality, it was nevertheless accepted that the impossibility of erasing personal data did not result in disproportionate interference, as the need to pro-

tect third parties and fair trading took precedence. This case has been criticised in legal scholarship for denying the right to be forgotten (Caravà, 2017, p. 292).

However, in *Luxembourg Business Registers* (on publishing the beneficial ownership of companies), the CJEU took a much restrictive approach and held that the disclosure of personal data on beneficial owners in the register was neither limited to what was strictly necessary nor proportionate to the objective pursued. This was especially the case because the provisions allowed disclosure of personal data which were not sufficiently defined and identifiable in these provisions; in addition, some optional provisions allowed the disclosure of personal data on condition of online registration, but were not in themselves able to demonstrate a proper balance or the existence of sufficient safeguards against the risk of abuse. In other words, the CJEU considered that the difficulty in defining the cases and conditions under which the general public can access information on beneficial owners could not justify the legislature's decision to grant access to the public as a whole (Cindori, 2023, p. 125). Such insufficient regulation can also lead to violation of the fundamental principles of administrative functioning (Štemberger Brizani, 2024, p. 162; Wegner, 2025, p. 28).

While in *Manni*, the CJEU held that it is proportionate to refuse to erase personal data in a commercial register after a company has ceased to exist, in *Agentsia po vpisvaniyata*, it took a different view. Specifically, faced with the situation that the register disclosed personal data not specifically and strictly required by law, the CJEU considered that this does not satisfy the 'necessity' requirement: it does not serve the objective of general interest and as such does not strike a fair balance between those objectives and data protection rights (Judgment of the CJEU, 2024). Another element criticised by the CJEU was the alleged lack of the Member State's administrative power to delete personal data. The CJEU ruled against the breach of the principle of prohibition of legal obstruction by institutions: the authority, in order to justify not erasing personal data, insisted that it does not review particulars (the personal data contained in the electronic images or originals of documents submitted to it), which were subject to a compulsory disclosure under Directive 2017/1132, before they are made available online, and therefore does not have the competence to erase anything. However, the CJEU ruled that the authority is the controller of the personal data and therefore is responsible for compliance with paragraph 1 of Article 5(2) of the GDPR (Judgment of the CJEU, 2024).

While in *Luxembourg Business Registers*, concerning personal data disclosed by private companies in a commercial register, the principle of transparency was not accepted by the CJEU as a justification, *Ministerstvo zdravotnictví* concerned public access to official documents in a public authority (not in a register). Therefore the principle of transparency was applicable and played a different and decisive role in balancing privacy. The CJEU held that, unlike in the case of commercial registers, there was a balancing of different interests: the public interest in scrutinising the public administration (Judgment of the CJEU, 2022) versus the right to protection of per-

sonal data. However, the problematic core identified in this context was the principle of proportionality: while Member States have the power to introduce national provisions to further specify data protection rules (Hamuľák, 2016; Maatsch, 2024), they also must ensure that the practical consequences, in particular of an organisational nature, arising from the additional requirements which they have laid down are not excessive (Judgment of the CJEU, 2025).

4.4. The 'objectives of general interest' criterion

In relation to the criterion of the 'objectives of general interest as recognised by the EU', the disclosure of personal data in commercial registers may serve various objectives, depending on the nature of the data. As identified in *Manni*, the objective can be the protection of third parties who are dealing with a company, in particular to identify the person authorised to bind the company. In *Luxembourg Business Registers*, it was identified that the data of beneficial owners may serve the objective of preventing money laundering and terrorist financing by creating, through increased transparency, an environment less likely to be used for these purposes. However, these objectives cannot be overgeneralised; each legal norm relating to the disclosure of certain elements or groups of personal data must have a specific objective of general interest. Additionally, in this context, the data subject must be able to reasonably expect their personal data to be processed for particular purposes (Jekabsone, 2023, p. 54). However, even though disclosing personal data in a register serves a specific objective of general interest, the possibility of using the data for purposes not envisaged by the legislation is an inherent risk of every public register (Lisičar & Jurić, 2024, p. 25).

Moreover, in this context, it is important to draw a red line between the public accessibility of activities of a public or of a private nature, such as the disclosure of company data in commercial registers. The general principle of transparency enshrined in Articles 1 and 10 TEU and Article 15 TFEU specifically covers activities of a public nature, such as the use of public funds, the work of public institutions, etc. By contrast, the information regarding the work of private companies, including their beneficial owners, is a distinct activity. Therefore, as established by case law, the principle of transparency as such cannot be considered an objective of general interest capable of justifying the interference which results from the general public's access to personal data held and disclosed by private companies in a commercial register (Judgment of the CJEU, 2022).

4.5. The 'appropriate, necessary and proportionate' criterion

Under the 'appropriate, necessary and proportionate' criterion, it is essential to examine, firstly, whether public access to information is appropriate for achieving the pursued objective of general interest; secondly, whether the interference with the fundamental rights resulting from such access is limited to what is strictly nec-

essary (in the sense that the objective could not reasonably be achieved as effectively by other means less prejudicial to the fundamental rights of the data subjects); and thirdly, whether that interference is not disproportionate to that objective, which implies in particular a balancing of the importance of the objective and the seriousness of the interference (Judgment of the CJEU, 2022).

- The following aspects have been relevant in case law so far when assessing the appropriateness, necessity and proportionality of personal data in a commercial register:
- The set of data made available is limited, clearly and exhaustively defined, and must be of a general nature in order to minimise potential prejudice (Judgments of the CJEU, 2017, 2022, 2025);
- Personal data is not stored longer than necessary (Judgment of the CJEU, 2017);
- There is opportunity to have derogation from disclosure in 'exceptional circumstances', on a case-by-case basis (Judgments of the CJEU, 2017, 2022);
- There is an absence of administrative restraints in compliance with the principles relating to the processing of personal data, such as the lack of competence of public authorities to erase personal data (Judgment of the CJEU, 2024);
- Personal data is provided on the condition of online registration in order to identify the person requesting that information (Judgment of the CJEU, 2022);
- Information is made available to the whole of society, even though the control of the matter is reserved to the competent authorities, and therefore these authorities or obligated entities should have access to personal data instead (Judgment of the CJEU, 2022);
- There is an absence of excessive national practical arrangements that undermine the content and objectives of data protection (Judgment of the CJEU, 2025).

While these aspects are relevant to commercial registers, this list, firstly, is by no means exhaustive, and, secondly, each aspect on its own is unlikely to undermine the 'appropriate, necessary and proportionate' criterion. Instead, compliance with it must be assessed on a case-by-case basis, and a higher risk exists when several of the above aspects have a cumulative effect. Also, while these aspects were analysed in the case law, new technology should be considered in the context of its dynamic nature and the potential for it to offer measures that cause less harm to privacy. While technology is generally seen as endangering privacy, the literature suggests that such technologies can also be used to protect it; these are known as 'privacy-preserving technolo-

gies' (Timan & Mann, 2021, p. 159). In the case of commercial registers, where data (including personal data) are available to any member of the general public, artificial intelligence can potentially be used for smart access control or risk-based data disclosure; for example, it could evaluate data requests and determine the level of detail that individuals should be allowed to access. This would provide all the information necessary for the objectives of general interest without full-scale public accessibility, thus balancing privacy rights. Currently, there is also a call in the legal literature for new, third-generation commercial registers that could automate more state functions and use more next-generation LegalTech solutions (Szostek et al., 2025, p. 182).

Once such privacy-preserving technologies are available, the case law relating to the 'appropriate, necessary and proportionate' criterion will need to be reconsidered, as the existence of these technologies means that the objective could reasonably be achieved effectively through other, less prejudicial means, with the available modern privacy-preserving technologies. Up to now, the CJEU has not examined the concept of privacy-preserving technologies under the 'appropriate, necessary and proportionate' criterion.

Conclusions

As was anticipated in the introduction of this article, the research shows that the CJEU has provided clear factors that controllers of commercial registers should take into consideration to avoid jeopardising fundamental rights, particularly with regard to privacy and data protection. The analysis of case law shows that while every dispute relating to commercial registers is at its core different, the CJEU has developed a general methodological approach to balancing public accessibility and privacy in such registers. Firstly, in these cases, the public accessibility that is considered an integral part of commercial registers is, from a methodological perspective, seen as an interference with the privacy of the individuals included in them. Secondly, all elements of the public accessibility of personal data must serve a clear objective of general interest, and consequently comply with different considerations of 'appropriateness, necessity and proportionality'. Thus, as claimed in the introduction, CJEU case law envisions that behind the public accessibility of commercial registers, individuals are entitled to claim their privacy.

Firstly, specifically in the case of commercial registers as administrative databases, it is important to underline that the general principle of transparency enshrined in Articles 1 and 10 TEU and Article 15 TFEU cannot be considered an objective of general interest capable of justifying the interference which results from the general public's access to personal data held and disclosed by private companies in a commercial register. While this principle covers public activities, such as the use of public funds, a declaration of private interests by officials in public positions or the

work of public institutions, it cannot be applied equally to commercial registers and information regarding the work of private companies.

Secondly, the case law on commercial registers is clear: the Achilles heel in such cases is typically the failure to consider whether it is 'appropriate, necessary and proportionate' (Potaičuks, 2024, p. 84) to make different elements of personal data subject to public accessibility in specific circumstances. In generalising the above-mentioned failures to balance privacy, two directions can be distinguished: the first serves to answer the question 'What is subject to public accessibility?', while the second addresses the question 'How is it subjected to public accessibility?' To be precise, the first direction is related to the type and extent of personal data in relation to the objective of general interest, while the second direction relates to the measures that minimise privacy damage or serve as a precautionary measure in relation to public accessibility. Examples of such measures include the opportunity to request derogation in 'exceptional circumstances', the activity of national authorities that minimises the negative impact on privacy, limitations on storage and the use of alternative technological solutions, such as online registration.

Commercial registers have come a long way. They have evolved from paper-based books kept by commercial courts that had to be visited in person to request data to powerful databases with lots of information available publicly online, thus causing new concerns and putting privacy under pressure. While public accessibility is an inherent feature of commercial registers today, the possibility of using this accessibility and the data they contain for purposes not envisaged by legislation is an inherent risk for every public register as well. This is an area in which privacy-preserving technologies, especially those offered by new AI-based opportunities, could transform the concept of public accessibility and balance the risks to privacy posed by it.

REFERENCES

Ayata, Z. (2024). European Union contracts in digital environments. In D.R. Troitiño (Ed.), *E-governance in the European Union: Strategies, tools, and implementation* (pp. 173–185). Springer Nature Switzerland.

Blajer, P. (2023). On the principle of public faith of land registers in a comparative context. *European Property Law Journal*, 12 (2–3), 79–125. https://doi.org/10.1515/eplj-2023–0005.

Caravà, E. (2017). Personal data kept in companies registers: The denial of the 'right to be forgotten'. *European Data Protection Law Review*, *3*(1), 287–292. https://doi.org/10.21552/edpl/2017/2/26

Cindori, S. (2023). Beneficial ownership – Demand for transparency, threat to privacy. *Review of European and Comparative Law*, *55*(4), 113–131. https://doi.org/10.31743/recl.16352

Costa, M. I. (2023). The legal concept of discrimination by association: Where does it fit into the digital era? *UNIO–EU Law Journal*, *9*(1), 16–28.

de la Guardia, R. M. (2005). La política europea de España después de su integración en las Comunidades. *Cuadernos europeos de Deusto*, *32*, 61–84.

European Parliament and Council. (2016, 27 April). On the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation) (O. J. L 119, 04.05.2016).

European Parliament and Council. (2017, 14 June). Directive (EU) 2017/1132 of the European Parliament and of the Council Relating to Certain Aspects of Company Law (Codification) (O. J. L 169, 30.06.2017).

European Union. (2007, 12 December). Charter of Fundamental Rights of the European Union (O. J. C 326, 26.10.2012).

Ferretti, F. (2022). A single European data space and data act for the digital single market: On datafication and the viability of a PSD2-like access regime for the platform economy. *European Journal of Legal Studies*, *14*, 173–218s.

Galetta, D.U., Hofmann, H. C. H., Lottini, M., Marsch, N., Schneider, J. P., Tidghi, M. (2014). Book VI – Administrative Information Management. In H. Hofmann, J. P. Schneider, & J. Ziller (Eds.). *ReNEUAL model rules on EU administrative procedure* (pp. 232–318). ReNEUAL research network on EU administrative law. https://hdl.handle.net/10993/19862

Garnowski, K. (2022). The principle of reliability of business trading in the context of personal changes in partnerships. *Review of European and Comparative Law 51*(4), 79–94. https://doi.org/10.31743/recl.14603

Gonet, W., & Wolska, H. (2019). Performing legal transactions based on entries in public registers: Selected issues. *Journal of Management and Financial Sciences*, *36*(1), 85–101. https://doi.org/10.33119/JMFS.2019.36.6

Hamuľák, O. (2016). *National sovereignty in the European Union: View from the Czech perspective*. Springer.

Heidemann, M. (2019). Commercial registers and transparency. *Amicus Curiae*, *112*(2017), 18–24. https://doi.org/10.14296/ac.v2017i112.5042

Jabłoński, M. (2025). The right to privacy and the obligation to transfer and authenticate personal data through the internet: Conflicting issues. *Bialystok Legal Studies*, *30*(4), 161–175. https://doi.org/10.15290/bsp.2025.30.04.10

Jekabsone, I. (2023). Selected legal issues in online adult education: Compliance of online learning and teaching process with GDPR. *TalTech Journal of European Studies*, *13*(2), 46–62. https://doi.org/10.2478/bjes-2023–0015

Judgment of the CJEU of 9 March 2017 on the case of *Manni*, C-398/15, ECLI:EU:C:2017:197.

Judgment of the CJEU of 22 November 2022 on the case of *Luxembourg Business Registers*, joined cases C-37/20 and C-601/20, ECLI:EU:C:2022:912.

Judgment of the CJEU of 4 October 2024 on the case of *Agentsia po vpisvaniyata*, C-200/23, ECLI:EU:C:2024:827.

Judgment of the CJEU of 3 April 2025 on the case of *Ministerstvo zdravotnictví*, C-710/23, ECLI:EU:C:2025:231.

Judgment of the Supreme Court of Latvia of 31 January 2019 in case no. SKA 148/2019 (A420322015).

Lisičar, H., & Jurić, M. (2024). How much transparency is too much? Open access to public registers in Croatia and personal data protection. *SEE Law Journal*, *13*(1), 12–31.

Kerikmäe, T., Troitiño, D. R., & Shumilo, O. (2019). An idol or an ideal? A case study of Estonian e-governance: Public perceptions, myths and misbeliefs. *Acta Baltica Historiae et Philosophiae Scientiarum*, *7*(1), 71–80.

Maatsch, A. (2024). Parliamentary adjustment during a crisis: Interplay of digitalization and domestic context factors. *Internet of Things*, *27*, 101316.

Mazur, V., & Ramiro Troitiño, D. (2024). The members of the EU and e-governance, analysis, and institutional support. In D.R. Troitiño (Ed.), *E-Governance in the European Union: Strategies, tools, and implementation* (pp. 39–55). Springer Nature Switzerland.

Mokrá, L. (2023). Digitally sovereign individuals: The right to disconnect as a new challenge for European legislation in the context of building the EU digital market. In D. R. Troitiño, T. Kerikmäe, O. Hamuľák (Eds.), *Digital development of the European Union: An interdisciplinary perspective* (pp. 189–197). Springer International Publishing.

Motzfeldt, H. M., & Næsborg-Andersen, A. (2018). Developing administrative law into handling the challenges of digital government in Denmark. *Electronic Journal of e-Government*, *16*(2), 136–146.

Mudrecki, A. (2021). The contemporary significance of the principle of proportionality in tax law. *Bialystok Legal Studies*, *26*(4), 37–51, https://doi.org/10.15290/bsp.2021.26.04.03

Outeda, C. C. (2024). The EU's AI Act: A framework for collaborative governance. *Internet of Things*, 27 (01291).

Papacharissi, Z., & Gibson, P. L. (2011). Fifteen minutes of privacy: Privacy, sociality, and publicity on social network sites. In S. Trepte, L. Reinecke (Eds.), *Privacy online: Perspectives on privacy and self-disclosure in the social web* (pp. 75–89). Springer Berlin Heidelberg.

Potaičuks, A. (2024). Data protection under review of constitutional court: Administrative databases directly accessible to public authorities. *TalTech Journal of European Studies*, *14*(2), 73–87. https://doi.org/10.2478/bjes-2024–0017

Potaičuks, A., & Tamužs, K. (2025). Open court principle and respecting privacy: Granting anonymity and restricting access to case files in constitutional court review procedure. *International Journal for Court Administration*, *16*(1), 1–14. https://doi.org/10.36745/ijca.593

Purtova, N. (2018). The law of everything: Broad concept of personal data and future of EU data protection law. *Law, Innovation and Technology*, *10*(1), 40–81. https://doi:10.1080/17579961.2018.1452176

Reichel, J., & Chamberlain, J. (2021). Public registries as tools for realising the Swedish welfare state: Can the state still be trusted? *Public Governance, Administration and Finances Law Review*, *6*(2), 35–52. https://doi.org/10.53116/pgaflr.2021.2.4

Rek, M. (2024). E-democracy in the EU. In D.R. Troitiño (Ed.), *E-governance in the European Union: Strategies, tools, and implementation* (pp. 103–115). Springer Nature Switzerland.

Škorić, S. (2020). The application of digital technology in business registration. *Pravo – teorija i praksa*, *37*, 1–12. https://doi.org/10.5937/ptp2004001S

Štemberger Brizani, K. (2024). Administrative contract in administrative matters: Slovenian law in comparative perspective. *Bratislava Law Review*, *8*(1), 153–168. https://doi.org/10.46282/blr.2024.8.1.717

Šulmane, D. (2025). Defense concept through the legislature – Protecting values for the sustainability of society. *Environment Technology Resources: Proceedings of the 16th International Scientific and Practical Conference*, *5*, 303–309. https://doi.org/10.17770/etr2025vol5.8511

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

Timan, T., & Mann, Z. (2021). Data protection in the era of artificial intelligence: Trends, existing solutions and recommendations for privacy-preserving technologies. In E. Curry, A. Metzger, S. Zillner, J. C. Pazzaglia, A. García Robles (Eds.), *The elements of big data value: Foundations of the research and innovation ecosystem* (pp. 153–175). Springer International Publishing.

Troitiño, D. R. (2022). The European Union facing the 21st century: The digital revolution. *TalTech Journal of European Studies*, *12*(1), 60–78. https://doi.org/10.2478/bjes-2022–0003

Troitiño, D. R., Mazur, V., & Kerikmäe, T. (2024). E-governance and integration in the European Union. *Internet of Things*, *27*(1), 101321. https://doi.org/10.1016/j.iot.2024.101321

van der Sloot, B. (2015). Do privacy and data protection rules apply to legal persons and should they? A proposal for a two-tiered system. *Computer Law & Security Review*, *31*(1), 26–45. https://doi.org/10.1016/j.clsr.2014.11.002

Vardanyan, L., Kocharyan, H., Hamulák, O., Mesarčík, M., Kerikmäe, T., & Kookmaa, T. (2023). The unwanted paradoxes of the right to be forgotten. *Masaryk University Journal of Law and Technology*, *17*(1), 87–109.

Wegner, J. (2025). The constitutionalization of the internet and the right to non-use. *Bialystok Legal Studies*, *30*(4), 28. https://doi.org/10.15290/bsp.2025.30.04.02

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

sciendo

DOI: 10.15290/bsp.2026.31.01.11

Received: 13.08.2025
Accepted: 13.12.2025

Celso Cancela Outeda
University of Vigo, Spain
ccancela@uvigo.gal
ORCID ID: 0000–0001–9034–2896

Óscar Briones Gamarra
University of Vigo, Spain
oscarbriones@uvigo.gal
ORCID ID: 0000–0003–3316–8670

Digital Transformation and Human Resources Planning in Public Administration: Insights from the Spanish Experience

Abstract: Digital transformation is reshaping public administration, especially in human resource management. This article explores how it redefines organisational values, skills, and roles, highlighting job evaluation as crucial for adapting to new digital demands. It also addresses HR planning challenges, stressing the need to anticipate future profiles and build a culture that embraces technological innovation to create a more agile and efficient administration.

Keywords: digitalisation, digital competencies, innovation, new professional profiles, remote working

Introduction

Digitalisation, which basically consists of the acquisition and implementation of technology, is a prerequisite for digital transformation. This involves a more profound modification or change that affects not only technology (ICTs), but also organisational culture, management models (administrative processes), and interaction with citizens in order to respond to their needs and expectations. The notion of digital transformation helps to understand the impact of digitisation, the implementation of which redefines the way we interact, work, and access public (and private)

services (Ayata, 2024; Kerikmäe et al., 2019; Mazur & Ramiro Troitiño, 2024; Ramiro Troitiño, 2022). Digital transformation brings about profound and extensive changes in public organisations that affect both their structure (how they are organised, their hierarchies, and the distribution of functions) and their functioning (procedures, decision-making, service provision, etc.) (Salvador Serna, 2021). Therefore public administrations, like other organisations, generate changes when they adopt technological tools, forcing them to comprehensively reconfigure their public management model (processes, structures, competencies, and values).

The human resources subsystem is deeply impacted by digital transformation, which requires updating public employees' training to develop digital skills aligned with today's technological demands (Salvador et al., 2020). Human resources planning (HRP) must also anticipate future professional needs, manage talent proactively, and enhance skills, structures, and performance. However, such planning is often informal and lacks professionalisation, relying on the discretion of senior officials or politicians. While not explored in depth here, digitisation enhances data-driven human resource management through AI, big data, and integrated systems, enabling better planning, evaluation, and training. It also demands new organisational standards, system interoperability, and updated methods, reshaping talent management in the public sector.

Two key points follow from the above. First, given that public employment represents a large share of the workforce in developed countries (Lupi et al., 2024; Niskanen, 1971), the planning and sizing of human resources deserve priority, especially in adapting to digital transformation (de la Guardia, 2005). Second, strategic management of public employment has a democratic role: amid growing scepticism about democracy, institutional legitimacy depends on delivering effective results (Easton, 1965). Assuming that public administration supports democratic development (Acemoglu & Robinson, 2012), this study sees improved HRP as a means to reinforce democracy.

After defining the concepts of digitalisation and digital transformation, this article aims to analyse their implications in the field of public administration, particularly in HRP. Based on an initial theoretical foundation, it refers to practices and values that emerge in the digital context, as well as the impact of these processes on the education and training of public employees. Next, it addresses some of the consequences of digital transformation on strategic HRP, with a special focus on identifying new professional profiles and adapting public employment to the demands of the digital environment, including remote working. The analysis is set in the Spanish context and seeks to contribute to a deeper understanding of the challenges and opportunities posed by talent management in the face of the digital transformation process.

1. Digital transformation and public administration: Evolving tools, services, and values

Mergel et al. (2019) outline three phases of digital transformation: digitisation (conversion of analogue services to digital formats and channels), digitalisation (process redesign through technology to enhance efficiency and accessibility), and digital transformation (which entails broader organisational, cultural, and relational shifts). This last phase represents a comprehensive rethinking of public services, grounded in user needs and policy analysis, and leading to both improved and entirely new digital services. As Trujillo Sáez & Álvarez Jiménez (2021) note, this transformation entails a reinvention of public administration to strengthen core values like efficiency, transparency, accountability, trust, and legitimacy.

Trujillo et al. (2021) emphasise that digital transformation arises from digitalisation, driving broad economic and social changes that impact organisations (Giovanola, 2023; Rek, 2024). However, adoption varies greatly across countries and regions, causing disparities in public service efficiency and quality. While some nations have advanced digital integration, others struggle due to poor infrastructure, resistance to change, and inadequate staff training (López et al., 2025; Poulose et al., 2024). Digital transformation positively influences strategy, culture, leadership, and human resources, enhancing strategic agility, but faces obstacles like infrastructure gaps, cybersecurity concerns, and skill shortages (López et al., 2025). This process affects all government levels – national, regional, and local – reshaping public service organisation and delivery (Hamuľák, 2016; Maatsch, 2024).

Pittaway and Montazemi (2020) argue that digital transformation entails redesigning key organisational processes, replacing outdated technologies, developing new skills, and introducing new working methods, leading to significant operational changes. This goes beyond technology adoption, involving structural and cultural reinvention within public organisations, and requiring shifts in the behaviours of both employees and citizens. Digital technologies improve efficiency and help institutions better meet challenges like transparency, agility, and personalised services. Thus digital transformation should be seen as a strategic and cultural change, where technology is a tool but managing organisational change is the real challenge.

Digital transformation deeply reshapes administrative processes to enhance agility, efficiency, and citizen focus. It promotes automation, simplification, and interoperability to enable accessible, personalised online services, replacing traditional face-to-face and paper-based models with faster, more transparent interactions. Workplace practices evolve through remote working and flexible office designs, changing task execution and professional interactions. These changes optimise internal management and transform citizen relationships, fostering a more efficient and accessible public service model (Salvador Serna, 2021). New workplace dynamics like remote working, task automation, and system interoperability are promoted. Public

employees need to develop digital skills, and organisations must implement change management strategies for smooth adaptation. The use of collaborative tools and data-driven decision-making, supported by technologies such as data analytics and AI, enables administrations to make more informed, evidence-based decisions beyond traditional methods.

Digital transformation fosters a citizen-centred approach that enhances proactivity, personalised service, and user satisfaction. It reshapes the relationship between administration and citizens by empowering the latter to participate actively, demand transparency, and access services directly. This raises citizens' expectations for faster, simpler public services, prompting administrations to modernise procedures, train staff, and build trust through accessible, efficient, and transparent services.

In short, digital transformation goes beyond technology, representing a comprehensive change that reshapes work practices, institutional values, and societal perceptions of public administration. As Salvador (2021) highlights, its success depends on strategic planning that integrates technological modernisation, staff training, and the fostering of an organisational culture aligned with digital-age challenges. Several authors (Ballart & Ramió, 2000; Cortés Abad, 2020, cited in Trujillo Sáez & Álvarez Jiménez, 2021; Mokrá, 2023; Rūse, 2014) underline the evident cross-cutting role of digital technologies in current public administration transformation policies.

Public administration must move beyond simply digitalising existing processes and services; it needs to harness the opportunities offered by digital technologies and data to fundamentally redesign operational models and its relationship with citizens. Specifically, three core dimensions of digital transformation can be identified: processes, technologies, and public servants. Each dimension includes key factors: processes involve policies, procedures, re-engineering, and computerisation; technologies cover data transmission, citizen interaction, and meeting needs; public servants encompass roles and responsibilities, training and innovation, and competencies (Salvador et al., 2020). Digital transformation is not merely technological upgrading but a structural and cultural shift that reshapes how administrations function and engage with society. Modernising technology alone does not ensure greater efficiency or improved public services; it requires a comprehensive strategy that integrates staff training and organisational change management.

2. Public employees and digital transformation: Redefining professional profiles in public administration

At the organisational level, digital transformation impacts four main areas: 1) the administration's structure, including governance type, unit size and organisation, resources, inter-institutional collaboration, and public–private partnerships; 2) the role of public employees, encompassing their mindsets, skills, and inter-organi-

sational networks of care; 3) leadership, which promotes learning from successfully transformed units, problem-solving, and resource mobilisation; 4) the distribution of power, particularly in decentralised contexts (Trujillo Sáez & Álvarez Jiménez, 2021).

In the context of digital transformation, human resources policies are crucial for organisational adaptation. Beyond the implementation of technology, staff must be trained to use it effectively, and the organisational culture must evolve. Trujillo Sáez and Álvarez Jiménez (2021) and López et al. (2025) emphasise the need for public employees to develop digital skills and receive ongoing training to meet new roles and responsibilities. For instance, Spain's National Digital Skills Plan (2021) recognises the unique digital training needs of public servants and proposes a dedicated programme to equip them for internal transformation, enabling the administration to fulfil its role in driving the country's digital transition (Trujillo Sáez & Álvarez Jiménez, 2021).

To meet the increasing expectations of digitally savvy users – particularly younger generations – public administrations must adopt technology to transform how they engage with citizens. This transformation begins with public servants, who are central to implementing these changes (Salvador et al., 2020). The widespread use of digital tools has significantly altered how governments operate and communicate, raising citizens' expectations for accessible, agile, and high-quality services. Consequently, it is crucial to reform recruitment and retention strategies to prioritise candidates with expertise in digital technologies, data analysis, and artificial intelligence. Additionally, performance evaluation systems should incorporate metrics that assess adaptability to digital environments and improvements in service quality.

Digital transformation necessitates a clear understanding of the digital competencies that current public employees must develop. This goes beyond simply learning to use new technologies; it involves grasping their broader impact on administrative workflows and service delivery. Key priorities for public administrations include promoting digital skills training programmes, fostering a culture of innovation that embraces technological solutions, and ensuring the recruitment of specialised talent in areas such as data analysis, artificial intelligence, cybersecurity, and digital platform development.

Finally, digital transformation in public institutions demands not only technical training but also a profound cultural shift (Criado Grande, 2016). This includes moving away from rigid hierarchical structures towards more collaborative and efficiency-driven work models. It involves challenging traditional mindsets that view digitalisation as a threat and replacing outdated bureaucratic procedures through automation and interoperability. A key obstacle in this process is resistance to change. To address this, public administrations must implement change management strategies, actively involve employees in the transformation, and emphasise the benefits for their daily work (Poulose et al., 2024). In this regard, when there is resistance to change in public organisations, it often works very well to clarify the purpose of these changes, eliminating uncertainties, socialise them among the workforce, and refining a good discourse from the leadership that motivates and rationalises the need for change.

In the context of digital transformation, public administrations must implement human resource management strategies that support staff in adapting to new digital tools and actively participating in the modernisation of the public sector. This process requires not only continuous training but also strategic workforce planning to identify which professional profiles will be essential, or redundant, in the future. The following analysis explores HRP within digital transformation, emphasising the challenges and opportunities it presents for public employment.

3. Human resource planning in the context of digital transformation

To properly understand the issue, it is important to recognise that public employment is not merely a structural matter but a subjective one (Pineda Nebot, 2019). It reflects political, economic, social, and cultural models tied to the concept of the public sector being managed (OECD, 2009). The characteristics, size, and structure of public employment often align with political ideologies ranging from more to less liberal views on the economy and public services. However, once a country defines its public sector model, the planning of public employment becomes a technical task which includes formalised human resource management processes such as job planning and analysis (Dolan et al., 2007).

Planning must be understood as both an essential (Cuenca Cervera, 2018) and a complex public function, given the significant resources and societal impact associated with public services and employees. In many developed countries, between 20% and 35% of public spending is allocated to staff salaries, with public administrations often being the largest employers (Knies et al., 2018; Pineda Nebot, 2019), representing an average of 20.8% of total employment in OECD nations (OECD, 2022). The concept of 'legitimacy through results' (Easton, 1965) or 'legitimacy through performance', in Weber's (2002) terms, remains central, as public service outcomes are directly tied to government actions and taxpayer contributions. Human resource management systems play a critical role in organisational performance (Knies et al., 2018). It is therefore important to distinguish between the political dimension of public sector size and the technical dimension of its management efficiency, with strategic planning falling under the latter. However, defining HRP is challenging due to the nature of public organisations as 'weak links', lacking clear, shared objectives (March & Olsen, 1976). This ambiguity undermines the strategic character of HRP, as a coherent strategy requires well-defined goals known throughout the organisation (Cuenca Cervera, 2018). Moreover, an absence of a long-term vision is exacerbated by the short-term focus of political agendas driven by electoral cycles (Salvador Serna, 2001, 2008).

The term *strategic* highlights the importance of aligning personnel decisions with the broader objectives of public administrations (Colley & Price, 2010; Cotten, 2007; Waterman et al., 1980). However, this planning function has often lacked profession-

alisation, becoming entangled in internal power struggles among departments and bureaucratic bodies (Salvador Serna, 2001; Sánchez Morón, 2012). Despite these challenges, HRP in public administrations is increasingly recognised as a strategic activity (Barzelay, 2006), requiring adaptability to changing environments (Mondy & Noe, 2005) and long-term vision (Bohlander & Scott, 2007). Strategic human resources planning, which is very common in the private sector, has traditionally been considered one of the main shortcomings of current public administrations. This traditional shortcoming is accentuated by the enormous complexity of the scope, diversity of tasks, and interests involved in any public administration (Salvador Serna, 2001).

This initial deficit in strategic planning (Gorriti Bontigui & Jiménez Asensio, 2018), traditionally justified by an incrementalist approach (Parrado Díez, 1996) and a context not conducive to rational resource use (Mayntz, 1985), complicates efforts to improve human resource management due to unclear starting points and time frames. Beyond these structural and technical limitations, there are operational challenges: departments often lack a clear understanding of their human resource needs, and personnel databases are frequently fragmented (Bouzas Lorenzo, 2011) or suffer from basic deficiencies (Cortés Carreres, 2001; Ferretti, 2022), resulting in duplicated data handling. However, this situation is gradually improving with the integration of big data technologies to support decision-making (Varela et al., 2023).

According to the classic definition by Vetter (1972), refined by Cuenca Cervera (2018), HRP is the process by which an organisation ensures it has a sufficient number of qualified staff in the right roles at the right time to enhance efficiency. This concept links organisational goals with the resources needed to achieve them. Cotten (2007) reinforces this idea by emphasising that HRP ensures the right people with the right skills are in the right job at the right time.

Building on Herrero (1995), HRP can be understood as a set of interrelated activities connected to various personnel subsystems (Bohlander & Scott, 2007), such as recruitment (to identify suitable candidates), training (to ensure up-to-date qualifications, especially in the context of digital transformation), and workforce management (to align staffing with workload demands). However, as Colley and Price (2010) note, many organisations lack sufficient data on their workforce – such as employee numbers, skills, and roles – which hinders effective planning and analysis.

The traditional lack of technical methods in HRP within public administrations can be attributed to several factors: the diversity and scale of public sector organisations (Albi et al., 1997; Salvador Serna, 2001), the fragmentation of units and agencies versus a need for centralised data (Colley & Price, 2010), and the absence of clear strategic objectives due to the political nature of public administration (Lohman, 2005, 2009). Often, political interests – regardless of party – favour informal and intuitive approaches to staffing decisions, complicating the development of strategic planning (Colley & Price, 2010; Salvador Serna, 2001). Nonetheless, there is growing consensus on the need for technical, objective workforce planning (Colley & Price, 2010),

as emphasised in Spain by the report of the Committee of Experts for the Study and Preparation of the Public Employee Statute (CEBEP, 2005). The following challenges are universally recognised as key obstacles to effective strategic HRP:

– The complexity and diversity of public administration
– Poor strategic orientation and a tendency towards intuitive processes
– The problem of incrementalism
– Deficiencies in personnel records
– The impact of corporatism

Conversely, based on these negative factors that affect proper planning, we can point to the features of a professionalised model or a correct way of planning. We can consider (Cuenca Cervera, 2010; Pineda Nebot, 2019; Villoria Mendieta, 1997) a series of activities that would necessarily be included in an HRP subsystem. These are sequentially arranged in the following list:

1) Planning of personnel stock (quantity and composition)
2) Planning of personnel needs (quantity and composition)
3) Planning of coverage strategy (specific objectives)
4) Evaluation of planning objectives and areas; projects for improvement (quantitative and qualitative redesign of positions)
5) Socialization and political-managerial leadership of planning

According to Poulose et al. (2024), digital transformation requires professionals to evolve and acquire new skills while collaborating with leadership to implement effective human capital strategies (Hill, 2019). For successful adoption, HR professionals must possess digital competencies and be familiar with relevant technologies, as these factors influence users' readiness to embrace new systems. However, HR departments often lag behind other areas in digital proficiency, which hampers digitalisation efforts (Mazurchenko & Maršíková, 2019). Additionally, HR professionals need strong data analytics capabilities – including statistical analysis, big data management for public decision-making (Varela et al., 2023), multivariate modelling, research methods, and qualitative data collection – along with the ability to formulate research questions and develop analytical models (Poulouse et al., 2024).

4. Planning personnel needs: New profiles for a new digital public service

The planning phase for personnel needs goes beyond numerical estimations and includes assessing professional suitability and qualification profiles, aligning with concepts such as 'competency-based management' (Alles, 2007) and 'human capital

management' (Bontis et al., 1999, p. 393). This phase also requires precision in identifying the specific positions to be filled and the urgency for them to be covered, forming part of a broader strategy for effective workforce planning.

Job evaluation is a strategic procedure in human resource management that is essential for advancing towards a more sophisticated management model. Its purpose is to assess the relative value of different roles within an organisation, which influences their placement in the staffing structure. This process enables the integration of emerging needs linked to digital transformation – such as digital communication, personalised technical support, cybersecurity, and complex technical procedures – into the job catalogue. As society evolves, so too must the skills and roles within the public sector. Once the need to depoliticise HRP and align it with professionalised planning is established, it is important to highlight the profound transformation underway due to the impact of new technologies on public administration.

As a result of the intense digitalisation process, current administrations need to adapt to a new technological environment. New trends in human resources management cannot ignore the constant impact on public administrations of new information technologies, digitalisation, big data, and AI, to mention just a few. These can be categorised and broken down into the following key areas.

4.1. The impact of digitalisation on processes

Digitalisation has significantly reduced the need for manpower in traditional administrative functions due to the streamlining of processes through e-government initiatives (Criado et al., 2004), robotic automation, and increased citizen participation. A notable example is the role private companies played in Spain during the rapid implementation of ERTEs (Temporary Employment Regulation Files) during the COVID-19 pandemic, effectively acting as processing agents. This shift illustrates how new technologies and automation are reshaping administrative operations. In this regard, examples of the introduction of new technologies and robotisation in the Administration include:

- Robotisation or automation of procedures: Automation has streamlined administrative tasks through interconnected databases across different government levels. For example, in Spain, verifying a person's legal residence, once a manual, paper-based process involving local police, is now handled digitally between the Ministry of the Interior and local administrations. Similarly, checks for tax or social security debts are now automated, reducing manual workload and increasing efficiency.
- Improvement of institutional websites as an official and reliable communication channel: In the case of Spain, the Tax Agency, the National Police, regional and local administrations, and the wide variety of health services that can be managed from the websites of the health departments of the different

autonomous communities stand out (Mahou Lago & Bouzas Lorenzo, 2012). Web forms have also been improved and simplified, and are now more intuitive, with simple and accessible information that is easily understandable by all types of users.

– Use of chatbots: The use of chatbots for recurring queries from public service users often replace the classic frequently asked questions or 'FAQs' sections. Examples in Spain include the Tax Agency and the public railway company (RENFE).
– Use of mobile applications ('apps') and smartphone features (WhatsApp, Telegram, SMS, etc.): Here, we can recall important meteorological phenomena in Spain in which these types of tools have played a major role, sometimes because of their usefulness in warning the population and ultimately saving human lives, and in other cases because their misuse and poor management of these warnings led to extreme weather events causing a significant number of human losses.[1]
– Massive introduction of fully telematic administrative procedures.

These changes in work processes bring up a clear debate, addressed extensively in Spain by Ramió and Salvador (2018), on the need to reformulate public sector staffing and design new standards of professional competence, in line with the logic of reducing the number of staff who 'row', and compensating for this reduction with staff who 'steer' (highly qualified and specialised personnel), if deemed necessary in each administration (Osborne & Gaebler, 1994). The exploration of new possibilities, in addition to being the focus of educational programmes, must be considered by training schools for public employees from the point of view of the production of intra-organisational knowledge that must flow through all parts of the institution (Bouzas Lorenzo & García Arias, 2007).

The protective role of the state must ensure that digital transformation does not exclude citizens lacking technological means or skills. This process must uphold values such as equity and the egalitarian purpose of public administration, avoiding the digital divide and ensuring, as European Commission state (2021), that 'no one is left behind'. In Spain, recent research highlights not only access issues but also digital complexity, with even young people struggling with procedures like obtaining a digital certificate (González-Cacheda et al., 2024).

1 In 2024, the DANA (*Depresión Aislada en Niveles Altos*, or isolated depression at high levels) phenomenon in Valencia was particularly striking in this regard. Despite the existence of such technological warning systems, significant shortcomings were observed in management and decision-making processes, which ultimately rendered the available alert technologies ineffective.

4.2. The impact of digital transformation on selection, provision, and ongoing training

Access

Selection processes, which clearly need improvement in Spain, are starting to develop the idea of accrediting prior digital skills (there is currently a debate about which model each administration should follow). The other option, whether complementary to certified accreditation or not, consists of demonstrating these skills through some type of test, which would normally be eliminatory in nature. However, this is beginning to be criticised due to its cost in terms of equipment, facilities, and test controls, with the idea of moving towards a system of prior accreditation of digital skills, or even demonstration of previous experience, gaining momentum.

On the other hand, civil service positions themselves seem to be at a critical juncture. The prevailing scientific doctrine in Spain predict the disappearance of civil service positions linked to activities that do not contribute public value, are easily replaceable, or will undergo intense robotisation in the performance of their tasks. At this point, it seems clear that alongside this movement of 'contraction' there is another of expansion, with an increase in STEM professions (professions linked to training in technical disciplines) and other profiles related to the digital revolution (MPTFP, 2021), such as data analysts, software developers, cybersecurity experts, and artificial intelligence experts, to name a few.

It is already possible to find examples in official gazettes that announce calls for applications for positions that reflect these new profiles, which are now considered structural even in the field of local government. This is the case of the Ayuntamiento de Guadalajara, which has advertised a position for a Communications and New Technologies Technician, and the Ayuntamiento de Finestrat (Alicante), which is looking to recruit a social media and communications technician.

Continuous retraining

Administrations are beginning to anticipate the need for constant updating of knowledge, with special attention to knowledge of computer environments or applications, given the enormous speed with which these contexts change. In this regard, special attention should also be paid to new forms of telematic relations between citizens and their administration (Salvador Serna, 2021), and within this, to the digital identity of users and the administration, with its various aspects in terms of security, accessibility, and usability of websites or telematic environments (Mahou Lago & Bouzas Lorenzo, 2012). This adaptation to new technological scenarios and procedures must be linked to opportunities for promotion, career advancement, or the provision of career destinations and jobs. In other words, adaptation to new ways of working in digital environments must be considered a professional merit, even though it also has a duty dimension: the duty of all public employees to keep up to date in their jobs, which is usually included in the civil service regulations of any

modern country. However, it should be noted that there may be excessive pressure on staff, who are subject to the intense pace of change in technological requirements and needs, making training and updating throughout their professional lives a source of stress and impairment in their personal and professional development. This causes a negative externality that is directly contrary to what is intended.

Training

Training in new technologies should be approached in a broad sense, with access to training being considered an obligation while at the same time being promoted, with a view to the ultimate goal of ensuring that such training permeates the entire organisation. It will be necessary to consider current and, above all, future skills (some of which are even unthinkable at this point), but it is possible to anticipate some basic skills that the profiles of public employees should have.

4.3. Process digitalisation and remote working

For some years now, human resource management theory has largely defended the possibilities of remote working in public administration, without any loss of productivity and even with the opposite effect. In fact, remote-working projects were already considered by the EU in 1993 as an important social phenomenon (European Union, 1993); they were and are presented with the characteristics of voluntariness, reversibility in both directions (company–employee) (AMC, 2002), adaptation to jobs where it can be implemented, the introduction of technical criteria for access to remote work, and objectives, and are offered with maximum transparency in the organisation. In a current definition, in this case taken from the relevant Spanish legislation (Real Decreto-ley 28/2020, 2020), remote work is 'carried out through the exclusive or prevalent use of computer, telematic, and telecommunications (ICT) means and systems'.

The first steps towards remote working as a project to be implemented in public administrations can be found in the European Framework Agreement on Teleworking, in the Lisbon Strategy (CES, 2007). This agreement, revised in 2009, seeks to promote 'e-government' to take advantage of new technologies by making information more accessible, structuring remote working around the basic principles discussed above (AMC, 2002). This first legal milestone was the result of a European initiative launched at the time to advance the development of this form of work organisation, based on articles 138 and 139 of the Treaty Establishing the European Community. It was founded on several key principles: remote working and returning to the workplace must be voluntary, and remote workers should receive equal treatment and rights to on-site employees, including collective representation, health and safety protections, training, and access to necessary work equipment.

Remote working aligns with and accelerates the digitisation of public administration and the shift towards hybrid work environments (Dixit, 2023). This trend builds on earlier European initiatives, including the 2010 Action Plan on eGovern-

ment (European Commission, 2010) and its predecessor from 2006. After the 2008 economic crisis, the Europe 2020 Strategy aimed for smart, sustainable, and inclusive growth, further supporting digital transformation. Although momentum has slowed in recent years, remote working has resurged, driven largely by the COVID-19 pandemic's unplanned and reactive push, and is now a key focus in debates on human resource management (Poulose et al., 2024).

Alongside organisational socialization, the citizen's perspective is crucial, and it is necessary to recognise the legitimate right of citizens to have their needs metand to the responsiveness of the public sector. As Sancho Royo (1999) highlights, citizens' contact with public administration remains fundamental, and this must be considered in remote working arrangements and broader digitalisation efforts, despite the well-documented benefits of online service delivery. The debate may be somewhat skewed: while face-to-face services remain highly valued by the public, growing evidence supports a dual-channel service-delivery model ('*two-way service*) that complements remote working. This model offers users both digital interaction and in-person assistance. A remote working approach compatible with maintaining face-to-face services seems the most suitable framework, considering all stakeholders in public service, as confirmed by González-Cacheda et al. (2024).

Data on remote working across Europe reveal that it is not the 'dream labour paradise' it was once thought to be. It is neither universally desired nor seen as a fully remote model where civil servants lose all in-person contact. Studies after the pandemic-forced shift show no clear preference for remote working among employees. Consequently, the future remote working model remains uncertain; clarity on its optimal extent, implementation challenges, and impacts on citizens in public administrations is awaited.

Based on original analyses conducted with over one hundred public employees since 2007, the following table summarises the key strengths, weaknesses, opportunities, and threats (SWOT) associated with the shift to remote working arrangements.

Table 1. Arguments for and against Remote Working.

For	Against
Lower environmental externalities (pollution), energy costs, and labour-related costs associated with the absence of the remote worker from public buildings.	Costs of equipment and connectivity; reliance on the remote worker's personal equipment unless the administration explicitly provides all necessary equipment.
Increased productivity in intellectual work, provided that a more isolated and focused environment is achieved at home.	Risk of reduced quality in public service provision (requires monitoring by the authority granting the remote work). In some cases, remote workers are expected to be permanently available and may be summoned to attend physically at any time.

Improved work–life balance, with knock-on benefits for the workplace climate (enhanced perception of the value of work and greater staff retention).	Loss of corporate identity or organisational socialisation (which can be mitigated by requiring at least one mandatory weekly day of in-person presence).
Potential for improved work efficiency through self-organisation.	Lack of direct supervision (which can be mitigated through technological tools or task-/goal-based performance techniques).
Motivation can be maintained through digital communication enhanced by the benefit of being allowed to work remotely.	Loss of motivational influence from the human team or hierarchical superiors, where these structures are present.
Social acceptance is possible if the greater oversight of remote working and the reduction in ecological footprint are properly communicated.	Lack of social acceptance, especially given the perception that public sector employment already enjoys favourable conditions.
Reduction in absenteeism due to improved compatibility between personal, family, and professional obligations.	–
Relocation of public administration jobs to rural or less advantaged areas.	Potential loss of collective learning.
Reduction in public expenditure associated with remote work (lower spending on electricity, heating, shared services staff, etc.).	Increased cost for citizens in terms of dissatisfaction with virtual service provision when compared to face-to-face attention.

Source: Author's own elaboration based on the reviewed literature and the SWOT methodology

An important issue is monitoring the quality and quantity of work under remote working arrangements. For remote working to gain social acceptance, productivity must be strictly controlled. Tools for tracking working hours, evaluating service quality, and monitoring performance are essential to demonstrate that remote working and productivity control are fully compatible.

Conclusions

This article has examined the impact of digital transformation on public administration, focusing particularly on strategic HRP. Digital transformation should be seen as an integrated process that goes beyond adopting technological tools (digitalisation), requiring the adaptation of people, processes, and organisational culture. It reshapes public administration by altering internal processes and citizen relationships. Automation, interoperability, and personalised digital services are replacing traditional, standardised, presence-based models; at the same time, a citizen-centred approach is gaining strength, enhancing participation, transparency, and service quality.

Digital transformation is reshaping the working environment through remote working, workspace reorganisation, and new organisational dynamics. Strategic HRP is directly affected, making investment in training, change management, and talent attraction essential. Public administrations must equip current staff to use dig-

ital tools and contribute to modernisation, while also identifying professional profiles that may be needed in the future or that may potentially become obsolete.

HRP encompasses activities like recruitment, training, and workforce allocation. Effective planning is hindered by the lack of accurate data on staff numbers, skills, and roles – a critical issue as public administrations face the challenges of rapid technological change. Emerging trends in people management must account for technologies like AI, big data, and automation, which are reshaping required job profiles and tools for strategic talent management.

Evidence shows that the new digital environment brings several challenges: a need for continuous training, 'technostress', reduced human interaction in service delivery, and the potential erosion of team spirit and organisational culture in remote work. These developments highlight the need to rethink HRP models and recruitment processes to align with evolving digital demands and to uphold core public sector values such as efficiency, transparency, accountability, and trust. At the same time, the debate on technological challenges has been enriched by proposals to address their impact on public organisations – particularly in HRP, but also in areas such as training, talent retention, organisational climate, personal development, and productivity monitoring in remote-work settings.

Finally, it is essential to reflect – drawing on scholarly evidence – on the impact of new work arrangements, especially remote working. Further research is needed on three levels: organisational dynamics, employee adaptation, and citizen satisfaction. This emerging line of inquiry carries major economic, social, political, and organisational implications, and requires a stronger empirical foundation.

REFERENCES

Acemoglu, D., & Robinson, J. A. (2012). *Why nations fail: The origins of power, prosperity, and poverty*. Crown Business.

Albi, E., González, J., & López, G. (1997). *Gestión pública. Fundamentos, técnicas y casos*. Ariel Economía.

Alles, M. A. (2007). *Gestión por competencias. El diccionario*. Granica.

AMC. (2002). *Acuerdo Marco Europeo sobre el teletrabajo*. https://ec.europa.eu/social/main.jsp?catId=521&langId=en&agreementId=1106

Ayata, Z. (2024). European Union contracts in digital environments. In Ramiro Troitiño, D., *E-governance in the European Union: Strategies, tools, and implementation* (pp. 173–185). Springer Nature Switzerland.

Ballart, X. & Ramió, C. (2000). *Ciencia de la Administración*. Tirant lo Blanch.

Barzelay, M. (2006). O estudo do desenvolvemento de estratexias nas organizacións gobernamentais; como integrar a xestión estratéxica e as teorías de prácticas sociais. *Revista Galega de Administración Pública ,, 1*(2), 9–25.

Bohlander, G., & Scott, S. (2007). *Administración de recursos humanos*. Thomson Learning.:

Bontis, N., Dragonetti, N. C., Jacobsen, K., & Roos, G. (1999). The knowledge toolbox: A review of tools available to measure and manage intangible resources. *European Management Journal*, *17*(4), 391–402. https://doi.org/10.1016/S0263–*2373*(99)00019–5

Bouzas Lorenzo, R. (2011). Sector público: Los recursos humanos en las administraciones públicas en España. In R. Gutiérrez & M. Martínez (Eds.), *Gestión de recursos humanos. Contexto y políticas* (259–278).. Thomson–Civitas 2011.

Bouzas Lorenzo, R., & García Arias, C. (2007, 10–14 July). *Detection of regional administration employee training needs in Spain: Developing an innovative methodology* [Conference presentation]. IAAS 27th International Congress of Administrative Sciences. Abu Dhabi. CD-ROM.

CEBEP. (2005). *Informe de la Comisión para el estudio y preparación del EBEP.* Instituto Nacional de Administración Pública – Ministerio de Administraciones Públicas.

CES. (2007). *Dictamen del Consejo Económico y Social sobre el Proyecto de real decreto por el que se regula el teletrabajo en la Administración General del Estado*. Mimeografiado.

Colley, L., & Price, R. (2010). Where have all the workers gone? Exploring public sector workforce planning. *Australian Journal of Public Administration*, *69*, 202–213. https://doi.org/10.1111/j.1467–8500.2010.00676.x

Cortés Abad, O. (2020). La Administración tras el coronabreak. Políticas para ¿un nuevo paradigma administrativo? *Gestión y Análisis de Políticas Públicas*, 24, 6–23. https://doi.org/10.24965/gapp.i24.10811

Cortés Carreres, J. V. (2001). Manual práctico de gestión de recursos humanos en la administración local. Dykinson.

Cotten, A. (2007). *Seven steps of effective workforce planning*. IBM Center for the Business of Government.

Criado, J.I., Fernández B, D., Olías de Lima G, M.B. (2004). *Construyendo la e-Administración Local*. Madrid. EuroGestion Pública.

Criado Grande, J. I. (2016). Las administraciones públicas en la era del gobierno abierto. Gobernanza inteligente para un cambio de paradigma en la gestión pública. *Revista de Estudios Políticos*, *173*, 245–275. https://doi.org/10.18042/cepc/rep.173.07

Cuenca Cervera, J. (2010). *Manual de dirección y gestión de recursos humanos en los gobiernos locales*. INAP.

Cuenca Cervera, J. (2018). Instrumentos de planificación de recursos humanos y selección: ¿Cambio de paradigma? *Revista Vasca de Gestión de Personas y Organizaciones Públicas*, Extra 2, 52–65.

De la Guardia, C. (2005). La historia en la era digital. *Ayer. Revista de Historia Contemporánea*, (58), 41–54. https://doi.org/10.55509/ayer/58–2005-03

Dixit R. (2023), "HR Trends for 2023: Future of Human Resource Management" Accessed online 25/6/23: https://www.selecthub.com/hris/hr-trends/#7

Dolan, S., Shuler, R., & Valle, R. (2007). *La gestión de los recursos humanos*. McGraw-Hill.

Easton, D. (1965). *A systems analysis of political life*. John Wiley & Sons.

European Commission. (2010). *Informe sobre la sociedad de la información europea para el crecimiento y el empleo*. https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=LEGISSUM:c11328

European Commission. (2021). *2030 Digital Compass: The European way for the Digital Decade* (COM/2021/118 final). https://eur-lex.europa.eu/legal content/EN/TXT/?uri=CELEX:52021DC0118

European Union. (1993). *Crecimiento, competitividad, empleo*. https://op.europa.eu/en/publication-detail/-/publication/4e6ecfb6–471e-4108–9c7d-90cb1c3096af/language-es

Ferretti, F. (2022). A single European data space and data act for the digital single market: On datafication and the viability of a PSD2-like access regime for the platform economy. *European Journal. Legal Studies*, *14*, 173–218.

Giovanola, B. (2023). Justice, emotions, socially disruptive technologies. *Critical Review of International Social and Political Philosophy*, *26*(1), 104–119.

González-Cacheda, B., Briones-Gamarra, Ó., & Varela-Álvarez, E. J. (2024). Atención telefónica y calidad percibida en los servicios de atención primaria en España. *Cuadernos de Gobierno y Administración Pública*, *11*(2), e97055. https://doi.org/10.5209/cgap.97055

Gorriti Bontigui, M., & Jiménez Asensio, R. (2018, 25 September). Mantener o transformar (gestión inteligente de vacantes en el empleo público del futuro). *Ensayo y Política*. https://rafaeljimenezasensio.com/2018/09/25/mantener-o-transformar-gestion-inteligente-de-vacantes-en-el-empleo-publico-del-futuro/

Hamuľák, O. (2016). *National sovereignty in the European Union: View from the Czech perspective*. Springer.Herrero, R. (1995). Los instrumentos de planificación. La oferta de empleo público. In B. Olías de Lima (Ed.), *La gestión de recursos humanos en el ámbito público,* 143–160 Complutense.

Hill, L. A. (2019). *Leading digital transformation* (HBS No. 420–043). Harvard Business School Publishing.

Kerikmäe, T., Troitiño, D. R., & Shumilo, O. (2019). An idol or an ideal? A case study of Estonian e-governance: Public perceptions, myths and misbeliefs. *Acta Baltica Historiae et Philosophiae Scientiarum*, *7*(1), 71–80.

Knies, E., Boselie, P., Gould-Williams, J., & Vandenabeele. W. (2018). Strategic human resource management and public sector performance: Context matters. *International Journal of Human Resource Management*, 35(14):1–13. https://doi.org/10.1080/09585192.2017.1407088

Lohman, M. C. (2005). A survey of factors influencing the engagement of two professional groups in informal workplace learning activities. *Human Resource Development Quarterly*, *16*(4), 501–527.

Lohman, M. C. (2009). A survey of factors influencing the engagement of information technology professionals in informal learning activities. *Information Technology, Learning, and Performance Journal*, *25*(1), 43–53.

López, A., Uquillas, G., Jácome, I., & Pérez, F. (2025). La transformación digital en la administración pública: evolución y tendencias de investigación. *Perspectivas Sociales y Administrativas*, *3*(1), 17–36. https://doi.org/10.61347/psa.v3i1.74

Lupi, A., Nolan-Flecha, N., & Handlos Thomassen, N. (2024). Size and composition of public employment: Data sources, methods and gaps. Towards improved internationally comparable data on public employment. *OECD Working Papers on Public Governance*, *76*. OECD Publishing. https://doi.org/10.1787/32c747be-en

Maatsch, A. (2024). Parliamentary adjustment during a crisis: Interplay of digitalization and domestic context factors. *Internet of Things*, *27*, 101316.

Mahou Lago, X. M., & Bouzas Lorenzo, R. (2012). Atención al usuario y comunicación en los portales web de salud autonómicos en España. *Gestión y Análisis de Políticas Públicas*, *8*, 99–113. https://doi.org/10.24965/gapp.v0i8.10005

March, J. G., & Olsen, J. P. (1976). *Ambiguity and choice in organizations*. Universitetsforlaget.

Mayntz, R. (1985). *Sociología de la administración pública*. Alianza Universidad.

Mazur, V., & Ramiro Troitiño, D. (2024). The members of the EU and e-governance, analysis, and institutional support. In Ramiro Troitiño, D. (Ed.), *E-governance in the European Union: Strategies, tools, and implementation* (pp. 39–55). Springer Nature Switzerland.

Ministerio de Política Territorial y Función Pública (MPTFP). (2021). *Orientaciones para el cambio en materia de selección en la Administración General del Estado*. https://funcionpublica.hacienda.gob.es/dam/es/portalsefp/secretaria-general-funcion-publica/Actualidad/2021/05/orientacionescambio.pdf

Mokrá, L. (2023). Digitally sovereign individuals: the right to disconnect as a new challenge for European legislation in the context of building the EU digital market. In Troitiño, David & Kerikmäe, Tanel & Hamulak, Ondrej. (Eds.). *Digital development of the European Union: An interdisciplinary perspective* (pp. 189–197). Springer International Publishing.

Mondy, R. W., & Noe, R. M. (2005). *Human resource management* (9th ed.). Prentice Hall.

Niskanen, W. A. (1971). *Bureaucracy and representative government*. Routledge.

OECD. (2009). *Government at a glance 2009*. OECD Publishing.

OECD. (2022). *Panorama de las administraciones públicas 2021*. OECD Publishing. https://doi.org/10.1787/1c258f55-es

Osborne, D. y Gaebler, T. (1994), La reinvención del gobierno. Ed. Paidós.

Parrado Díez, S. (1996). *Las élites de la administración estatal (1982–1991): estudio y pautas de reclutamiento*. Instituto Andaluz de Administración Pública.

Parrado Díez, S. (2002). *Sistemas administrativos comparados*. Tecnos.

Pineda Nebot, C. (2019). Retos de futuro en la gestión de los recursos humanos públicos en España. *Administração Pública e Gestão Social*, *11*(4), 1–19.,

Pittaway, J. J., & Montazemi, A. R. (2020). Know-how to lead digital transformation: The case of local governments. *Government Information Quarterly*, *37*(4), 101474. https://doi.org/10.1016/j.giq.2020.101474

Poulose, S., Bhattacharjee, B., & Chakravorty, A. (2024). Determinants and drivers of change for digital transformation and digitalization in human resource management: A systematic literature review and conceptual framework building.

Management Review Quarterly 75(3) 1911–1936 . https://doi.org/10.1007/s11301–024-00423–2

Ramió, C., & Salvador, M. (2018). *La nueva gestión del empleo público: Recursos humanos e innovación de la administración*. Ediciones Tibidabo.

Real Decreto-ley 28/2020, de 22 de septiembre, de trabajo a distancia [Royal Decree-Law 28/2020, of September 22, on remote work]. (2020). *Boletín Oficial del Estado*, (253). https://www.boe.es/eli/es/rdl/2020/09/22/28

Rek, M. (2024). E-democracy in the EU. In Ramiro Troitiño, D. (eds). *E-governance in the European Union: Strategies, tools, and implementation* (pp. 103–115). Springer Nature Switzerland.

Rūse, I. (2014). Nordic–Baltic interaction in European Unio negotiations: Taking advantage of institutionalized cooperation. *Journal of Baltic Studies*, *45*(2), 229–246.

Salvador, Y., Llanes, M., & Suárez, M. A. (2020). Transformación digital en la administración pública: ejes y factores esenciales. *Avances*, *22*(4), 590–602. http://www.ciget.pinar.cu/ojs/index.php/publicaciones/article/ view/573/1635/

Salvador Serna, M. (2001). El papel de las instituciones en la gestión de las administraciones públicas. *Revista del CLAD Reforma y Democracia*, *20*, 1–19,.

Salvador Serna, M. (2008). Nuevas tendencias en gestión de recursos humanos en las administraciones públicas: ¿Están cambiando las reglas del juego? *Revista Internacional de Organizaciones*, *1*, 109–127.

Salvador Serna, M. (2021). Transformación digital y función pública: capacidades institucionales para afrontar nuevos retos. *Documentación Administrativa*, *8*, 25–42. https://doi.org/10.24965/da.i8.11030

Sánchez Morón, M. (2012). *La administración tras la crisis: el empleo local* [Conference presentation]. XII congreso sobre recursos humanos en el sector público. Vitoria.

Sancho Royo, D. (1999). *Gestión de servicios públicos: estrategias de marketing y calidad.* Tecnos.

Troitiño, D. R. (2022). The European Union facing the 21st century: The digital revolution. *TalTech Journal of European Studies*, *12*(1), pp. 60–78.

Trujillo Sáez, F., & Álvarez Jiménez, D. (2021). Transformación digital de la administración pública: ¿Qué competencias necesitan los empleados públicos? *Gestión y Análisis de Políticas Públicas*, *27*, 49–67. https://doi.org/10.24965/gapp.i27.10923

Varela, E., Briones, O., & González, B. (2023). La gobernanza de la salud a partir de la gestión de la evidencia: análisis de la toma de decisiones sanitarias en el caso de la pandemia COVID-19 en Galicia. (2020–2022) [Special issue]. *Revista Vasca de Gestión de Personas y Organizaciones Públicas*, *5*, 80–105. https://doi.org/10.47623/ivap-rvgp.06.2023.AB.05

Vetter, E. W. (1972). The nature of long range manpower planning. In M. J. Matteson, R. N. Blakeney, & D. R. Domm (Eds.), *Contemporary personnel management: A reader* (pp. 94–103). Canfield Press.

Villoria Mendieta, M. (1997). Modernización administrativa y gobierno posburocrático. In E. Bañón & R. Carrillo (Eds.), *La nueva administración pública,* 77–104. Alianza.

Waterman, R. H., Jr., Peters, T. J., & Phillips, J. R. (1980). *Structure is not organization*. *Business Horizons*, *23*(3), 14–26. https://doi.org/10.1016/0007–6813(80)90027–0

Weber, M. (2002). *Economía y sociedad*. Fondo de Cultura Económica.

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

sciendo

DOI: 10.15290/bsp.2026.31.01.12

Received: 21.07.2025
Accepted: 13.12.2025

Lucia Mokrá
Comenius University Bratislava, Slovakia
lucia.mokra@fses.uniba.sk
ORCID ID: 0000–0003–4883–0145

Digitalisation of the EU Healthcare System: Member States Enabling the European Health Data Space[1]

Abstract: This article presents a comprehensive overview of the legislative and policy frameworks adopted at the EU Member State level in healthcare systems and analyses the development of their implementation regarding the 2030 digital targets. The comparative analysis of national strategies for the digitalisation of health services aims to provide information on the existence of the framework for digitalisation of the sector and on the implementation of the e-health record system, and to assess the feasibility of achieving the goal in each Member State and in a cumulative way for the European Union and its Digital Decade Policy Programme. The output of the analysis is an essential contribution to the current process of creating a common European health data space, for which the creation of an e-health information system that is digital and shareable is a prerequisite for interoperability, while ensuring digital inclusion for everyone.

Keywords: digitalisation, health records, access to public services, citizens' rights, policy frameworks, European Health Data Space

Introduction

The European Union, similarly to other international organisations, states and non-state authorities, has been facing challenges connected to the technological development and digitalisation of the 21st century (Kováčiková, 2020). To address the

1 This paper is the outcome of research carried out under the Jean Monnet Network: European Network on Digitalisation and E-Governance (ENDE) project. The primary data on national e-health strategies were collected with the support of research assistant Laura Klingová.

digital challenges for a human-centred, sustainable and prosperous digital future, the EU has strategically set its targets and objectives related to digital transformation by 2030 in the Digital Decade Policy Programme (European Commission, 2022).

The programme is based on four pillars, of which one focuses on digitalisation of public services. Within that, three main goals have been set: all key public services will be available online, all citizens will have access to medical records online, and all citizens will have access to digital ID. Regarding the EU-level trajectories of 2024[2], it is necessary to annually assess development in these concrete areas, focusing on the nationwide availability of online services for citizens to access their electronic health records data and the percentage of individuals that can obtain or make use of their own minimum set of health-related data. According to a Eurobarometer survey on the Digital Decade published in 2023, a significant majority of respondents (76%) expect digital technologies to have a decisive impact on access to and uptake of healthcare services by 2030 (e.g. telemedicine and artificial intelligence in disease diagnosis), even in EU countries where patients are not actually resident. A minority of respondents (13%) think that their country should prioritise citizens' access to their electronic health records between now and 2030 (Eurobarometer, 2023).

While several studies exist assessing the impact of healthcare systems across the Member States, these have mainly focused on the efficiency and effectiveness of the systems and their implementation with the support of European funds. The Commission's assessment, in a case study on the digitalisation of health, provides an overview of initiatives that have been launched and provided with grants and loans through the Recovery and Resilience Facility (European Commission, n.d.a.), but is limited to five Member States.

This article analyses how one of the main objectives of the Digital Decade Policy Programme is addressed, namely the digitalisation of public health services. The core tool analysed is access to, or the creation of, an e-health records system within a national digitalised service system. For this purpose, I analysed in which strategic and policy documents Member States have planned an e-health system, focusing on the creation of an e-health records system, which I considered a strategic digital tool for the effective provision of healthcare, as well as a tool for inclusion and preventing discrimination (Mee et al., 2025). Beyond that, I focus on the implementation of an e-health system, based on the strategic national policy or legal document and its compliance with the ambition of the EU to achieve the Digital Decade programme target of having an e-health records system in all Member States by 2030, which is a precondition for non-discriminatory and effective access to digitalised health services and the creation of health IDs.

2 The paper analyzes data available as of December 31, 2024, as the reference point preceding the adoption of the relevant legislation for the European Health Data Space Regulation.

1. Digitalisation of healthcare

The European Commission presented its vision for a digitally transformed Europe by 2030 in the communication '2030 Digital Compass: The European way for the Digital Decade' (European Commission, 2021), followed by the other two strategic documents: the Digital Targets for 2030 (European Commission, 2022) and the Digital Decade Policy Programme (European Commission, 2023b). The Digital Decade lays down a vision for digital transformation. As detailed in the inter-institutional solemn declaration on digital rights and principles for the digital decade, the following rights are suggested: putting people and their rights at the centre of the digital transformation; supporting solidarity and inclusion; ensuring freedom of choice online; fostering participation in the digital public space; increasing the safety, security and empowerment of individuals; and promoting the sustainability of the digital future. These rights are expected to complement existing rights in the context of digitalisation and are intended to empower citizens in navigating the digital landscape and to provide guidance for EU Member States and other stakeholders (European Commission, 2022).

In the light of the continuously digitalising environment and following the Digital Decade, the Commission adopted the European Declaration on Digital Rights and Principles for the Digital Decade, underlining a human-centred digital transformation (European Commission, 2022). The declaration is anchored in the EU treaties and the EU Charter of Fundamental Rights as well as the case law of the Court of Justice of the EU. It aims to serve as an overarching reference framework for digital transformation in Europe, based on the principle that EU rights and freedoms, as well as European values, should be respected online in the exact same way they are offline. More specifically, the declaration promotes rights and principles relevant for the digital transformation, i.e. putting people and their rights in the centre, fostering solidarity and inclusion, guaranteeing freedom of choice online, promoting participation in the digital public space and ensuring the sustainability of the digital future (Kerikmäe et al., 2019; Mazur & Ramiro Troitiño, 2024; Ramiro Troitiño, 2023). The European Declaration on Digital Rights and Principles offers citizens a bridge to the Union's digital laws and policies, as it indicates the direction of travel of the Union on its journey to digital transformation (Costa, 2023; European Commission, 2022; Outeda, 2024). As outlined in this Declaration, above all, the EU institutions commit to facilitating and supporting seamless, secure and interoperable access across the EU to digital public services designed to meet people's needs in an effective manner, including digital health and care services, notably access to electronic health records (European Commission, 2022, section A7c).

As part of the Digital Decade, Member States are encouraged to ensure that 100% of key public services are online, with 100% access to e-health records and 80% digital ID usage by citizens by 2030 (European Commission, 2022). With pub-

lic services, including health services, increasingly moving to a digital mode, Member States are called on to ensure that nobody is left behind. Additionally, as many argue, digitalisation of healthcare may increase the risk of digital exclusion (Kwiatkowska & Skorzewska-Amberg, 2019). The phenomenon of digital exclusion is generally associated with the lack of skills necessary for using information technologies and can lead to social isolation (Kwiatkowska & Skorzewska-Amberg, 2019). Access to these services is a right of all EU citizens, regardless of age, gender or disability, as specified in the right to non-discrimination in Article 21 of the Charter of Fundamental Rights.

Although the European Commission adopted the Digital Decade programme in 2023, some of the EU Member States adopted their national strategic goals for digitalisation earlier, and an important part of the assessment is whether and to what extent these are compliant with the European strategic policy goals and values adopted later. Overall, the focus of this paper is to provide analytical insight into the EU Member States' obligation to fulfil the goals set in the Digital Decade programme, as well as to ensure that the fundamental principle of the EU law on non-discrimination is applied in healthcare in a way which is compliant with the principles of subsidiarity and proportionality. As Mee et al. (2025) have argued, digital exclusion leads to marginalisation and inequality. According to the UN (UNGA HRC, 2018), digital inclusion can be characterised as a basic human right. Therefore, it is essential to provide safeguards to access healthcare, including e-health systems implementing digitalisation simultaneously to create the European Health Data Space (EHDS), which will benefit all EU citizens, including patients, healthcare professionals, researchers, policymakers and industry players (European Union, 2025). However, I must also underline that the research combines two policies of regulation and implementation in consecutive periods which only partially overlap. Hence the research topic may raise additional questions, such as the use of digital platforms, protection of personal data, governance structure and requirements for network and information systems, which are not addressed or analysed here.

The research uses a tailor-made approach to the specific topic of the nexus of digitalisation in e-health, analysing the EU Member States' approaches to the required digitalisation with the stated 2030 targets, and its application in the area of healthcare, based on the EHDS Regulation adopted in 2025 which foresees full implementation by 2035 (including access by third parties and international organisations). The e-health records system is considered a strategic research point, and can be used as a pilot study for assessment of the preparedness of EU Member States for the full implementation of the EHDS Regulation and the creation of a European Health Union.

2. E-health and digitalisation: The contemporary challenge to a clash of competences?

When analysing e-health policies, we need to clarify the framework of competences for health policy and digitalisation. According to Article 168 of the Treaty on the Functioning of the European Union (TFEU), a 'high level of human health protection shall be ensured in the definition and implementation of all Union policies and activities' (European Union, n.d.). Based on the principle of subsidiarity and proportionality, the EU's role in health policy is therefore complementary to national policies (de la Guardia, 2005; Giovanola, 2023; Hamuľák, 2016; Maatsch, 2024). Although the EU treaties do not contain specific provisions on digitalisation, the European Commission can take appropriate action, in close coordination with Member States, under sectoral and horizontal policies to promote innovation, economic growth and the development of the single market (Ayata, 2024; Ferretti, 2022).

An important fact that needs to be outlined before the analysis is that the Digital Decade targets by 2030 are political goals, which became strongly supported by financial resources through the Recovery and Resiliency Facility of the European Union that addressed the impact of the Covid-19 pandemic (European Commission, n.d.b). Given the experience of the pandemic period, and also regarding the lack of Union competences in close coordination of health policies and instruments but especially health information exchange, 2024 was also significant in terms of strengthening cooperation and competences. The Council of the EU and the European Parliament have reached a preliminary agreement on new legislation facilitating the exchange of and access to health data at the EU level (Council of the European Union, 2024).

On 21 January 2025, the Council adopted a new law that makes it easier to exchange and access health data at the EU level. The European Health Data Space Regulation aims to improve individuals' access to and control over their personal electronic health data, while also enabling certain data to be used for research and innovation purposes for the benefit of patients. It provides for a health-specific data environment that will ensure cross-border access to digital health services and products within the EU. Under the new rules, individuals will have faster and easier access to electronic health data, regardless of whether they are in their home country or another Member State; they will also have greater control over how that data is used. EU countries will be required to set up a digital health authority to implement the new provisions. Currently, the level of digitalisation of health data in the EU varies from one Member State to another, making it more difficult to share data across borders. The new EHDS Regulation requires all electronic health record systems to comply with the specifications of the European electronic health record exchange format, ensuring that they are interoperable at the EU level (Council of the European Union, 2025).

The EU Regulation is phasing its implementation, with several transition periods. While the Commission is obliged to adopt several key implementing acts pro-

viding for the operationalisation of the regulation, EU Member States have already been implementing some of the instruments, such as electronic health records, as they are interlinked with the 2030 digitalisation targets. While the legal obligations of EU Member States in relation to the use of health data in the categories of medical records and genomic data are foreseen as being fully implemented in the EU by 2031, this paper provides an analytical insight into the implementation of e-health records at the EU Member State level, as potential examples of the effective, gradual and structured transition foreseen by the Regulation.

3. The e-health records system in the digital strategies of Member States and its implementation

The initial analysis focused on the existence of a digital strategy or action plan which provides access to public services and particularly to health services. While I can confirm that all 27 Member States do have a digital strategy or action plan in place, only 15 currently have a focused digital strategy in the area of healthcare (Table 1). It is important to add that Denmark also has their Digital Health Strategy 2018–2022, which has contributed to the implementation of an e-health system in practice (Danish Health Data Authority, n.d.).

Table 1. National digital healthcare strategies

Country	National policy framework
Austria	eHealth Strategy Austria
Belgium	Act of 21August 2008
Bulgaria	National Strategy for E-health and Digitalisation of the Healthcare System 2030
Croatia	National Health Development Plan for the Period 2021–2027
Czech Republic	National e-Health Strategy of the Czech Republic
Germany	Digitalisation Strategy for Health and Care
Hungary	Digital Healthcare Development Strategy
Ireland	Harnessing Digital – The Digital Ireland Framework
Latvia	Digital Health Strategy to 2029
Malta	A National Health System Strategy for Malta 2023–2030
Poland	Strategy of the e-Health Centre for 2023–2027
Portugal	Portuguese e-Health Strategy
Slovenia	e-Health for a Healthier Society
Spain	Digital Health Strategy
Sweden	Draft Roadmap for a National Digital Infrastructure for Healthcare

Source: author's own processing

Reviewing the EU Member States' frameworks, it can be confirmed that most Member States have established a policy framework within the digital strategy for the implementation of an e-health records system. A comprehensive framework which could provide comparable data for the EHDS is not fully in place, however, and the national systems providing online access services for citizens to access their health data vary. This full and universal compliance is considered as the realisation of the e-health principles, which in 2022 was on average 64% in the EU 27; in 2023 it was 79% (European Commission, 2023a; European Commission, 2024).

The Commission's evaluation results for 2023 (considering data up to 31 December 2022) and 2024 (considering data up to 31 December 2023) show that countries are progressing well in facilitating citizens' access to electronic health records. Twenty-two Member States (81%) improved in score in the past year. The top five countries in the EU 27 with the most developed systems are Belgium (100%), Denmark (98%), Estonia (98%), Lithuania (95%) and Poland (90%). The biggest improvement over the previous year was observed for France (+25 points), Portugal (+23 points), Slovakia (+20 points) and Germany (+17 points). Additionally, 17 Member States (63%) made improvements by either providing more categories of health data or providing the available data in a timely manner (European Commission, 2024; Table 2).

Table 2. E-health records system development score by EU Member State

Country	e-health records system		Country	e-health records system	
	2023	2024		2023	2024
Austria	88%	88%	Italy	71%	83%
Belgium	85%	100%	Latvia	79%	85%
Bulgaria	77%	77%	Lithuania	92%	95%
Croatia	86%	86%	Luxembourg	67%	76%
Cyprus	70%	68%	Malta	78%	88%
Czechia	47%	51%	Netherlands	69%	72%
Denmark	96%	98%	Poland	86%	90%
Estonia	89%	98%	Portugal	63%	86%
Finland	90%	83%	Romania	57%	59%
France	54%	79%	Slovakia	42%	66%
Germany	70%	87%	Slovenia	80%	88%
Greece	61%	74%	Spain	83%	85%
Hungary	80%	86%	Sweden	70%	78%
Ireland	0%	11%			

Source: European Union, 2024

Following this evaluation of the policy framework, it is essential that these indications of strategic policy settings are not only implemented but also considered in detail. Since 2023, the Commission has published a Digital Decade status report and country-focused reports about the target of online access to electronic health records for European citizens (Rek, 2024; Rūse, 2014). In the 2024 report, the Commission evaluated the progress made by EU Member States regarding citizens' access to their electronic health records. Methodologically, a composite indicator has been used for this monitoring, incorporating four layers that analyse multiple aspects of access to e-health records: the implementation of electronic access services for citizens, categories of accessible health data, the access technology used (eID or access via portals or apps), coverage (by population and healthcare providers) and equitable access opportunities (European Commission, 2024). Out of all EU Member States, 16 were above the EU average of 64% in 2023; currently, 17 are above the average of 75% in 2024 (Table 3).

Table 3. E-health data by EU Member State (access to electronic results and reports)

Country	Score in health data		Country	Score in health data	
	2023	2024		2023	2024
Austria	87%	87%	Italy	60%	80%
Belgium	52%	100%	Latvia	74%	86%
Bulgaria	48%	48%	Lithuania	87%	92%
Croatia	92%	92%	Luxembourg	48%	51%
Cyprus	92%	83%	Malta	92%	100%
Czechia	38%	43%	Netherlands	21%	23%
Denmark	92%	92%	Poland	58%	60%
Estonia	100%	100%	Portugal	67%	83%
Finland	87%	74%	Romania	38%	37%
France	37%	68%	Slovakia	27%	88%
Germany	69%	69%	Slovenia	100%	87%
Greece	60%	79%	Spain	66%	81%
Hungary	77%	92%	Sweden	69%	91%
Ireland	65%	5%			

Source: European Union, 2024

The European Commission evaluated the performance of the Member States in enabling citizens' access to e-health data, highlighting the role of five so-called 'leader countries' in digitalisation of health data: Belgium, Denmark, Estonia, Lithuania and Poland. While other countries were classified as fast-trackers (scoring between 83 and 88%) or followers (scoring between 66 and 79%), the Commission also highlighted three countries where digitalisation of health data is very low: Romania, the

Czech Republic and Ireland (European Commission, 2024). It should also be added here that while the Czech Republic has a specific strategy for digitalisation in the health sector, neither Romania nor Ireland has such a strategic document. The adoption of a specific document or action plan would reinforce awareness of the need to digitalise access to health information and at the same time enable its effective implementation to achieve the set digitalisation targets by 2030.

Conclusions

This comparative overview highlights the need to enhance the digitalisation of health services across all 27 EU Member States. With the progress of the new EHDS Regulation, effective and harmonised digitalisation of services in the health area as well as e-health records in all Member States are not only the targets by 2030, but also a necessity for the implementation of the exchange of health information, better access to health services and the improvement of the well-being of all EU citizens.

In order to digitalise and meet the objectives of the digital programme, all EU Member States have adopted national digital plans and programmes. However, some of them have also adopted a specific digital health strategy to digitalise health services in more detail and in a more effective way. In the European Commission's assessment, out of the five so-called 'leader countries', four had a specific strategy for digitalisation in health services, including the goal of having an e-health records system in place. Establishing a strategic framework and then implementing effective tools, including sufficient financial resources (European Commission, n.d.b.), are three key factors for successful implementation, not only now but also for achieving the 2030 targets. Considering the progress of EU Member States' e-health records development scores, which increased in the last two years in all countries (see Table 2), we can identify positive development in this area that is compliant with the key parts of the EHDS Regulation, including the first group of priority categories of health data in all EU Member States before March 2029. Furthermore, we can also in later stages verify to what extent Member States are on track with the implementation, ensuring patients have fast and free access to their own electronic health data, are not digitally excluded and that security and privacy protection is in place. The e-health system and access to electronic health records should significantly reduce the administrative burden and allow health professionals to provide effective and patient-centred care.

REFERENCES

Ayata, Z. (2024). European Union contracts in digital environments. In D. Ramiro Troitiño (Ed.), *E-governance in the European Union: Strategies, tools, and implementation* (pp. 173–185). Springer Nature Switzerland.

Costa, M. I. (2023). The legal concept of discrimination by association: Where does it fit into the digital era? *UNIO–EU Law Journal*, *9*(1), 16–28.

Council of the European Union. (2024, March). *European health data space: Press release*. https://www.consilium.europa.eu/sk/press/press-releases/2024/03/15/european-health-data-space-council-and-parliament-strike-provisional-deal/

Council of the European Union. (n.d.). *EU health policy*. Retrieved 25 January 2025, from https://www.consilium.europa.eu/en/policies/eu-health-policy/

Danish Health Data Authority. (n.d.) *Digital health strategy 2018–2022: The e-health system implementation*. Retrieved 25 January 2025, from https://sundhedsdatastyrelsen.dk/digitale-loesninger

de la Guardia, R. M. (2005). La política europea de España después de su integración en las Comunidades. *Cuadernos europeos de Deusto, 32*, 61–84.

Eurobarometer. (2023, December). *European citizens and the 'Digital Decade'*. https://europa.eu/eurobarometer/surveys/detail/2959

European Commission. (2021). *2030 Digital Compass: The European way for the Digital Decade*, COM(2021)118 final. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52021DC0118

European Commission. (2022). *Digital citizenship: Rights and principles for Europeans*. https://digital-strategy.ec.europa.eu/en/policies/digital-principles

European Commission. (2023a). *Digital Decade e-Health indicators development: Annexes*. https://op.europa.eu/en/publication-detail/-/publication/1da67c3e-461d-11ee-92e3–01aa75ed71a1/language-en

European Commission. (2023b, 5 January). *Digital Decade Policy Programme 2030*. https://digital-strategy.ec.europa.eu/en/library/digital-decade-policy-programme-2030

European Commission. (2024, 2 July). *Digital Decade 2024: eHealth indicator study*. https://digital-strategy.ec.europa.eu/en/library/digital-decade-2024-ehealth-indicator-study

European Commission. (n.d.a). *Case study on the digitalisation of health (eHealth)*. Retrieved 20 January 2025, from https://commission.europa.eu/document/download/652a3175-d410–4608-8f0e-642049433c35_en

European Commission. (n.d.b). *Europe's Digital Decade: Digital targets for 2030*. Retrieved 27 January 2025, from https://commission.europa.eu/strategy-and-policy/priorities-2019–2024/europe-fit-digital-age/europes-digital-decade-digital-targets-2030_en

European Union. (2024). *2024 Digital Decade ehealth indicator study: Annex – country factsheets*. Publications Office of the European Union. https://data.europa.eu/doi/10.2759/276133

European Union. (2025). Regulation (EU) 2025/327 of the European Parliament and of the Council of 11 February 2025 on the European Health Data Space and Amending Directive 2011/24/EU and Regulation (EU) 2024/2847 (Text with EEA relevance) (O. J. L 2025/327, 05.03.2025). http://data.europa.eu/eli/reg/2025/327/oj

European Union. (n.d.). *Treaty on Functioning of the European Union*. Retrieved 31 January 2025, from https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:12012E/TXT:en:PDF

Ferretti, F. (2022). A single European data space and data act for the digital single market: On datafication and the viability of a PSD2-like access regime for the platform economy. *European Journal of Legal Studies*, *14*, 173–218.

Giovanola, B. (2023). Justice, emotions, socially disruptive technologies. *Critical Review of International Social and Political Philosophy*, *26*(1), 104–119.

Hamuľák, O. (2016). *National sovereignty in the European Union: View from the Czech perspective*. Springer.

Kerikmäe, T., Ramiro Troitiño, D., & Shumilo, O. (2019). An idol or an ideal? A case study of Estonian e-governance: Public perceptions, myths and misbeliefs. *Acta Baltica Historiae et Philosophiae Scientiarum*, *7*(1), 71 – 80.

Kováčiková, H. (2020). A definition of digital markets by the Slovak Antimonopoly Office: Has the boat to digitalisation already sailed? *Yearbook of Antitrust and Regulatory Studies*, *13*(21), 247–258. https://yars.wz.uw.edu.pl/images/yars2020_13_21/YARS_13_21.pdf

Kwiatkowska, E. M., & Skorzewska-Amberg, M. (2019). Digitalisation of healthcare and the problem of digital exclusion. *Journal of Management and Business Administration Central Europe*, *27*(2), 48–63.

Maatsch, A. (2024). Parliamentary adjustment during a crisis: Interplay of digitalization and domestic context factors. *Internet of Things*, *27*, 101316.

Mazur, V., & Ramiro Troitiño, D. (2024). The members of the EU and e-governance, analysis, and institutional support. In D. Ramiro Troitiño (Ed.), *E-governance in the European Union: Strategies, tools, and implementation* (pp. 39–55). Springer Nature Switzerland.

Mee, P., Gussy, M., Huntley, P., Kenny, A., Jarratt, T., Kenward, N., Ward, D., & Vaughan, A. (2025). Digital exclusion as a barrier to accessing healthcare: A summary composite indicator and online tool to explore and quantify local differences in level of exclusion. *Universal Access in the Information Society*, *24*, 1425–1437.

Outeda, C. C. (2024). The EU's AI Act: A framework for collaborative governance. *Internet of Things* 27(3), 101291.

Ramiro Troitiño, D. (2023). EU elections and internet voting (i-voting). In D. Ramiro Troitiño, T. Kerikmäe & O. Hamuľák (Eds.), *Digital development of the European Union: An interdisciplinary perspective* (pp. 319–333). Springer International Publishing.

Rek, M. (2024). E-democracy in the EU. In D. Ramiro Troitiño (Ed.), *E-governance in the European Union: Strategies, tools, and implementation* (pp. 103–115). Springer Nature Switzerland.

Rūse, I. (2014). Nordic–Baltic interaction in European Union negotiations: Taking advantage of institutionalized cooperation. *Journal of Baltic Studies*, *45*(2), 229–246.

United Nations General Assembly Human Rights Council (UNGA HRC). (2018). The promotion, protection and enjoyment of human rights on the internet, A/HRC/RES/38/7. https://digitallibrary.un.org/record/1639840?v=pdf

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

sciendo

DOI: 10.15290/bsp.2026.31.01.13
Received: 22.07.2025
Accepted: 08.01.2026

Nicole Smith
University of Bologna, Italy
nicole.smith3@studio.unibo.it
ORCID ID: 0009–0005–3338–9221

How Do Anti-Money Laundering Laws Affect the Growth of Fintech Lending Platforms in Europe?

Abstract: The aim of this study is to explore the effects of anti-money laundering (AML) legislation on fintech lending platforms in the European context, focusing on the balance between protecting market integrity and safeguarding the expansion of innovation in the financial field, a tension that is encapsulated by the innovation trilemma. By analysing the current state of fintech lending and the evolving anti-money laundering regulatory landscape in Europe, the paper investigates how rigid compliance requirements can unintentionally suppress innovation. Furthermore, it discusses how these challenges can be overcome and assesses potential solutions, such as regulatory sandboxes and innovation hubs. The study concludes that AML rules are essential to strengthen financial stability; however, a more harmonized and technologically adaptive regulatory approach is necessary to promote innovation without compromising risk mitigation. Strengthening international cooperation and taking advantage of digital regulatory tools could be key in determining the future of fintech compliance and sustainable growth.

Keywords: fintech lending, EU AML laws, financial supervision, legal compliance

Introduction

The rapid growth of financial technology (fintech) has dramatically transformed the financial landscape, offering innovative solutions that increase the accessibility, efficiency, and competitiveness of financial services. Fintech lending platforms in particular have developed new ways for individuals and small businesses to access credit and avoid traditional banking systems. However, the digital nature of fintech also introduces risks, mostly concerning financial crimes such as money laundering. Given the increasing importance of these platforms, effective regulatory frameworks

are essential to ensure that financial markets remain stable, secure, and transparent (Arner et al., 2016; Kou & Lu, 2025; Wang, 2023).

This paper explores the impact of anti-money laundering (AML) laws on the growth and operations of fintech lending platforms in Europe. The research question at the core of this investigation is: 'How do AML regulations affect fintech lending platforms, and what implications do these regulatory requirements have for the platforms' growth, operations, and development?'. I specifically focus on AML laws because they directly address one of the most critical risks faced by the fintech sector. Although there are already various regulatory frameworks governing the financial sector, such as the Payment Services Directive (PSD2), they primarily concern open banking and competition, whereas fintech lenders.[1]

Focusing on AML laws is particularly relevant because the European Union (EU) has recently updated its AML framework in response to the rising risks associated with digital finance and cross-border transactions. This regulatory environment presents a dual challenge for fintech lenders: on the one hand, they must ensure compliance with stringent AML requirements, and on the other, they must maintain their ability to innovate and compete in the rapidly evolving financial market. This paper aims to assess how these regulations affect the ability of fintech lenders to grow and operate effectively in the European market, highlighting the complexities and trade-offs involved.

The significance of this topic lies in the balance of innovation and regulation. Fintech lending has contributed to greater financial inclusion and the diversification of credit markets; nonetheless, its rapid growth has placed fintech lenders under the scrutiny of governments and regulators. As highlighted by Berg et al. (2021), examples such as the Woolard Review on unsecured consumer lending in the UK and the Chinese government's decision to restructure Alipay demonstrate how regulatory attention intensifies with the expansion of fintech activities.[2] At the same time, the regulatory burden, particularly in terms of AML compliance, can create significant challenges for start-ups and scale-up, as noted by the European Banking Authority (2025), and even the careless use of innovative compliance technologies can expose firms to heightened risks of money laundering and terrorist financing. Thus understanding the implications of AML laws for this sector is pivotal for policymakers, regulators, and industry stakeholders seeking to protect innovation while ensuring market integrity and security.

1 The Payment Services Directive (PSD2), Directive (EU) 2015/2366 of the European Parliament, is a law that promotes payment security and innovation, and facilitates third-party access to bank accounts for new payment services.

2 The Woolard Review was published in 2021 and is a report commissioned by the UK's Financial Conduct Authority to assess the unsecured credit market. The Chinese Central Bank issued a decision on January 2023 to change Alipay, a popular payment app, to having no actual controller.

The structure of this paper is as follows: in the first section, an overview of the fintech lending environment in Europe will be provided, while in the second part, a summary of the current EU AML regulatory framework, focusing on the key directives and regulations, will be presented. The third section will discuss the challenges fintech lenders face in complying with AML laws, particularly the impact on business operations and growth, exposing the main concerns raised by the literature. The concluding section will explore potential policy recommendations to improve the regulatory environment for fintech lending platforms and will underline the importance of finding a balance between overregulation and innovation, before closing with a summary of key findings and considerations for the future development of the fintech lending sector.

1. Overview of fintech lending

This section provides a general overview of the fintech lending market, including its various models and the key drivers of its growth. Fintech is defined as 'technologically enabled innovation in financial services that could result in new business models, applications, processes, or products with an associated material effect on financial markets and institutions and the provision of financial services' (Carney, 2017). This broad definition captures the impact of fintech on traditional financial systems.

Fintech development has followed different paths globally. As described by Langley and Leyshon (2020), in the Global North fintech focuses on 'transforming banking'; in contrast, in the Global South it aims at 'banking the unbanked'. In Africa, the sector has converged on mobile money; in East and South Asia, there is an intertwining of African-style 'bottom of the pyramid' retail fintech and western-style B2B innovation. Regions such as the Middle East, West and Central Asia, and Latin America are considered to be late starters in fintech; most fintech capital raising by fintech has occurred in China, where the sector stands out in terms of its size, history, and qualitative features. Runners-up to China are the US, the UK, and a few other countries, including EU Member States such as the Netherlands, Germany, Latvia, and Estonia, in per capita fintech investment and in terms of the capital raised by fintechs (Wójcik, 2020). According to Baba et al. (2020), the extensive network of formal financial service providers in Europe is the cause of the lower penetration of certain fintech services, as well as a preference for cash in some countries, like Italy, and the heterogeneity of regulations across jurisdictions.

Fintech lending is categorized based on two key factors (Berg et al., 2021): the nature of the interaction between customer and lender, and the technology used for borrower assessment and monitoring (Giovanola, 2023). A lending process is considered fintech-driven when the entire interaction between borrower and lender occurs through digital platforms, eliminating the need for face-to-face meetings or physi-

cal documentation (Kerikmäe et al., 2019; Mazur & Ramiro Troitiño, 2024; Troitiño, 2023). This approach significantly reduces processing times, lowers operational costs, and improves the user experience, making credit more accessible and efficient. The screening and monitoring process falls under the fintech umbrella when lenders use advanced technology such as big data analytics, machine learning (ML), and artificial intelligence (AI) to improve traditional risk-assessment models. These technologies enable lenders to expand the range of data sources (e.g. digital footprints, transaction histories, and behavioural data) or extract deeper insights from existing information, leading to more accurate credit risk evaluations (Costa, 2023; Ferretti, 2022).

Since traditional banks increasingly adopt digital solutions, the distinction between fintech lenders and traditional financial institutions has become less clear. Many banks now offer fully digital loan applications and use alternative data sources to assess creditworthiness, mirroring fintech capabilities. To maintain a clear differentiation, researchers (Cornelli et al., 2020; Gopal & Schnabl, 2022; Lentini et al., 2025) often introduce additional classification criteria, for example by stipulating that fintech lenders operate independently of incumbent banks or by excluding firms that accept deposits, as deposit-taking is typically associated with traditional banking institutions.

Baba et al. (2020) identify four main business models for lending used by fintech companies:

– peer-to-peer lending;
– crowdfunding;
– the balance sheet model and the mixed model;
– and invoice trading.

Peer-to-peer (P2P) lending is the most prominent business model in Europe; it works by directly matching borrowers and investors (lenders). P2P lending emerged nearly two decades ago with the goal of democratizing financial services, enabling borrowers to access funds without the involvement of traditional financial institutions. Initially, P2P platforms served as a decentralized marketplace where individual lenders funded loans to individual borrowers, effectively bypassing banks (Suryono et al., 2019).

Crowdfunding platforms are in many aspects similar to P2P lending because they provide a digital marketplace for matching investors and entrepreneurs. Different types of crowdfunding models exist: rewards crowdfunding, where the entrepreneur grants a reward to those who financially support the launch of a business concept or service; equity crowdfunding, where the investor receives shares in a company; and real-estate crowdfunding, where the backer can acquire ownership of a property through the purchase of shares in properties (Wangchuk, 2021).

The balance sheet model entails the fintech company originating the loan and assuming the credit risk associated with it. This kind of lending is the closest to bank lending, where the fintech company obtains debt or equity funding and records the loans in its balance sheet, however without deposit funding. This model is rarely run by itself and is often combined with other models. For example, some platforms initially adopt the balance sheet model and abandon it once they have established their reputation, shifting to a marketplace model relying solely on retail or institutional investors. However, according to the Cambridge Centre for Alternative Finance (2017), a good number of platforms continue using their own balance sheet alongside retail and/or institutional investors even after gaining a reputation. Finally, invoice trading platforms are similar to P2P lending platforms, with individual invoices used as collateral for loans. The invoice is sold on the platform, and multiple investors can buy slices of it. All of the above-mentioned fintech business models share several similarities, including a high degree of automation, as previously discussed, with the use of AI and ML, and a focus on convenience and simplicity in the customer experience, with a digitally active and younger customer base.

The growth of fintech credit is driven by multiple factors, which can be broadly classified into supply-side drivers (factors influencing lending platforms) and demand-side drivers (factors influencing borrowers and investors). The Committee on the Global Financial System & Financial Stability Board (2017) has identified and listed these factors. On the supply side, the fintech credit industry has flourished thanks to technological advancements in computer power, data storage, and mobile connectivity, which have enabled the automation of lending processes. Moreover, unlike traditional banks, fintech lenders have the ability to scale, benefiting from low marginal costs and the capability to expand rapidly through digital identification and standardized contracts (Ayata, 2024; Outeda, 2024). They have also been able to fill market gaps left by banks, such as micro-business lending and other high-risk and underserved markets, which create opportunities for fintech firms to step in (Mokrá, 2023). On the demand side, the shift in consumer preferences and investor behaviour has further stimulated fintech lending. Consumers now expect high speed, convenience, and lower costs in financial services. There have also been generational shifts: digital-savvy millennials and Gen Z consumers are more likely to prefer online lending solutions compared to older generations. This preference was particularly strengthened after the 2008 financial crisis, which weakened consumer trust in traditional banks, making alternative lending platforms more attractive.[3] Finally, network effects are especially important in this context: the more investors join fintech platforms, the more borrowers are drawn in, creating a self-reinforcing cycle of growth.

3 'Millennials' refers to individuals born between approximately 1981 and 1996, while 'Gen Z' refers to those born from 1997 onwards.

Despite its rapid growth and its numerous advantages, fintech lending is not without its difficulties. Since banks have been building up their digital banking activities, there could be competition between incumbent lenders and fintech activities. However, there have also been examples of cooperation between the two, e.g. the partnership between the British arm of the Santander bank and the American fintech platform Kabbage to accelerate automated SME lending.[4] In addition, many fintech lending platforms have not yet experienced a full economic cycle, including major financial downturns or a recession; thus it is uncertain how they will perform during such periods of economic stress because they have not established risk-management practices and regulatory protections. In this regard, the regulatory framework surrounding them is complex and ever-changing across different jurisdictions. It is particularly relevant to understand the factors that have driven the growth of fintech lending, as they provide context for analysing how regulatory measures, particularly AML laws, impact its development and future trajectory in Europe.

2. Anti-money laundering (AML) regulations in Europe

As defined by the EU, money laundering is 'the conversion of the proceeds of crime into apparently clean funds, usually via the financial system, for example by disguising the sources of the money, changing its form or moving the funds to a place where they are less likely to attract attention' (European Union, 2015, Chapter 1, Section 1(1)(3)(a)). AML therefore refers to the set of laws, regulations, and procedures aimed at preventing criminals from concealing illegally obtained funds or assets. AML measures help to identify, track, and report suspicious financial activities.

With globalization and digital advancements, fintech has made cross-border transactions faster and more efficient. However, it has also created new avenues for money laundering due to fewer intermediaries, decentralized digital currencies, and anonymity-enhancing technologies (Omotoso, 2024). On one side, fintech can enhance AML detection through the integration of advanced technologies such as AI, ML, and blockchain; on the other, its risks demand stronger regulatory oversight to prevent abuse. The EU has been combating money laundering since 1991, with the adoption of the initial Anti-Money Laundering Directive on the prevention of the use of the financial system for the purpose of money laundering (Council of the European Communities, 1991), which has undergone multiple revisions. These directives set out measures to establish the true identity of customers, report suspicious transactions, and set up preventive systems within organizations. Among other things, entities subject to the Directive are required to identify and verify the identity of their

4 UK SMEs can access Santander's new working capital solution, offering funding approval between £500 and £100,000 within minutes and access within a day, using the Kabbage platform to accelerate automated lending.

customers (customer due diligence) and of beneficial owners (the person who ultimately owns or controls the legal entity or arrangement, on whose behalf a transaction is being carried out), and to monitor their business relationship with customers. The third AML Directive (European Union, 2005) emphasized the requirement to assess and mitigate money-laundering risks based on the customer's profile and his/her business relationships and transaction patterns; the fourth AML Directive (European Union, 2015) made these risk assessments mandatory both at the national and the institutional level. More recently, EU Regulation 2023/1113 (European Union, 2023) has further amended Directive 2015/849 (European Union, 2015), significantly reshaping AML supervision, particularly in relation to crypto-assets, by expanding the scope of supervision, licensing requirements, and subject entities (Tomczak, 2025).

The regulatory environment has changed over time to address new risks and emerging trends. The 2020 AML Action Plan (European Commission, 2020) identified weaknesses in the existing system and led to a comprehensive AML legislative package. A central part of this package is the latest regulation, Regulation 2024/1624 (European Union, 2024b), commonly known as the AMLR, which will apply from July 2027. It establishes harmonized AML rules, replacing the previous minimum standards. Furthermore, it introduces stricter due diligence measures for crypto-asset service providers (CASPs), as well as expanding the list of obliged entities to include, amongst others, football agents and clubs.

The sixth AML Directive (European Union, 2024c) aims to address the inconsistencies and divergences between the Member States' approaches to AML. This Directive expands the definition of the criminal offence of money laundering to include aiding, abetting, inciting, and attempting to commit it. Moreover, it mandates CASPs to conduct due diligence for transactions above EUR 1000 and strengthens financial intelligence units (FIUs) and cross-border information exchange.[5] Additionally, Regulation 2024/1620 (European Union, 2024a) introduces the EU AML Authority (AMLA), which is located in Frankfurt and will be operational from 2028. This organization directly supervises high-risk financial entities and strengthens coordination among national regulators. The establishment of the AMLA signifies a step toward centralized AML enforcement; literature has highlighted the importance of a harmonized system and strong coordination as a prerequisite for an effective AML legal apparatus (Arnone & Borlini, 2010).

Turning to the concrete implications of AML laws for fintech lenders, Article 3 of the AMLR defines financial institutions, credit intermediaries, crowdfunding service providers, and credit institutions, among others, as 'obliged entities'. Fintech lenders are not explicitly outlined as a separate category under the EU AML framework, but they generally fall under broader financial classifications depending on their business

5 FIUs are national agencies responsible for receiving, analysing, and sharing financial information related to money laundering and terrorist financing to support law enforcement actions.

model and licensing. For example, P2P lending platforms or those facilitating financing through investor contributions can be categorized as crowdfunding service providers and therefore must comply fully with AML requirements. Indeed, under the EU (2020) Crowdfunding Regulation, a fintech platform that facilitates the granting of loans (P2P lending) or is involved in placing transferable securities and transmitting client orders for crowdfunding purposes is classified as a crowdfunding service provider. Thus, the AMLR does not define fintech lenders explicitly, but it includes broad financial service categories that likely cover them. As a result, fintech lenders must implement robust AML measures, including customer due diligence, transaction monitoring, and reporting of suspicious activities, which will be further investigated in the following section.

3. The impact of AML regulation on fintech lending platforms and possible solutions

As mentioned, the European AML regulatory framework has significant implications for fintech lending platforms, which are therefore required to conduct thorough customer due diligence, 'know your customer' checks, and reporting of suspicious activity, all of which can delay onboarding and transaction processing. This makes fintech lenders less attractive for customers, due to lengthy verification which may worsen the user experience. Moreover, the lenders must also bear the costs of integrating sophisticated solutions to adhere to these requirements; for example, by collecting sensitive customer information there is a need to build robust data protection measures to prevent breaches, not only to comply with AML regulations, but also with data privacy laws such as the GDPR.[6] The risk-based approach requires specific due diligence based on the customer's risk level, which can also slow operations, especially for high-risk clients. Transaction monitoring and data retention requirements necessitate significant investments in systems to detect suspicious activities and maintain records for at least five years, increasing operational costs. Finally, for platforms operating internationally, the need to comply with varying AML rules across jurisdictions adds complexity: fintech companies must invest in comprehensive research to understand the regulatory environment of each jurisdiction they operate in, including staying updated on legislative changes and emerging compliance trends. Although these rules are crucial to combat money laundering, they create significant barriers for fintech lenders, reducing their ability to scale quickly, innovate, and provide uniform services to customers.

6 The GDPR (2016) is a regulation in EU law on data protection and privacy in the European Union and the European Economic Area. It governs the collection, storage, and processing of personal data to ensure that individuals' privacy rights are upheld.

Finding a balance between market integrity, rules simplicity, and innovation is the core principle behind the innovation trilemma theorized by Brummer and Yadav (2017), which suggests that regulators can only effectively achieve two out of these three goals at any given time. In the context of fintech lending, market integrity is essential; however, ensuring it often comes at the cost of rule simplicity. AML regulations, especially when applied across multiple jurisdictions, can be complex and difficult for fintech lenders to handle, particularly for smaller or new firms without extensive legal resources. These complexities may be an obstacle to the platform's ability to innovate because their resources are diverted toward compliance instead of technological advancement. As a result, financial innovation, the key driving force behind fintech, can be limited by the heavy burden of compliance with AML regulations. To balance this, regulators might create rules that are clear and easy to follow, but at the risk of oversimplifying or overlooking unique aspects of fintech operations, potentially weakening market protections. As Brummer and Yadav (2017) highlight, current regulatory frameworks tend to place paramount focus on market integrity and squeeze out innovation.

Regulatory sandboxes can be a solution to this, offering fintech lenders a controlled environment to test and refine AML compliance solutions under supervisory oversight, enabling innovation while ensuring adherence to regulatory standards. However, regulatory sandboxes do not guarantee a direct path to full market entry, despite creating an avenue for experimentation. At the European level, the main initiative in place is the European Blockchain Regulatory Sandbox (2023–2026), which focuses on public-sector use cases through the European Blockchain Services Infrastructure; however, this might limit its relevance to the private-sector fintech industry. Moreover, the AI Regulatory Sandbox (2024) allows companies, including fintechs using AI for risk assessment and fraud detection, to test AI-driven financial solutions under regulatory supervision. Nonetheless, they are not specifically dedicated to fintech and instead focus on broader areas. Some EU countries (such as Poland's KNF or the UK's FCA Regulatory Sandbox) operate regulatory sandboxes at a national level, but this means that fintech firms must navigate different national sandboxes, leading to regulatory inconsistency, which makes it harder for start-ups to scale across the EU (Hamuľák, 2016; Maatsch, 2024).

The majority of European countries set up innovation hubs, schemes whereby regulated or unregulated entities can work with competent authorities on fintech-related issues and seek non-binding guidance on the conformity of innovative financial products, services, business models, or delivery mechanisms with licensing, registration, and/or regulatory requirements (ESMA, 2018). According to authors like Buckley et al. (2019) and Roide (2022), innovation hubs should be prioritized over regulatory sandboxes, or where those already exist, they should be integrated into an innovation hub. Innovation hubs may be more cost-effective and versatile than regulatory sandboxes. While the latter have the advantage of offering a structured test-

ing environment, many of their benefits are already provided by innovation hubs at a lower cost and with greater flexibility. Nonetheless, as highlighted by Bartnik (2025), even innovation hubs are not without their shortcomings: in many cases they provide only limited avenues for engagement and are restricted to submitting questions to supervisors or contacting email addresses for general inquiries. Furthermore, the criteria for defining eligible participants in innovation hub programmes remain ambiguous, and frequently rely on vague and broadly defined terminology.

Conclusions

The rapid evolution of fintech lending presents both opportunities and challenges in the fight against money laundering. In Europe, fintech companies' development is on the rise but has not progressed as rapidly as in other regions. This can partly be explained by the high preexisting banking presence but also by burdensome regulations, unlike in jurisdictions such as China and the USA. As emphasized by Lagarde (2018), attention must be given to the balance between regulatory stringency, which safeguards consumers and investors, and the flexibility needed to foster financial innovation that benefits the public responsibly and sustainably. AML regulations are crucial for maintaining market integrity, but they must not suppress financial innovation. The innovation trilemma proposed by Brummer and Yadav (2017) further stresses the fragile balance regulators must strike between financial innovation, market integrity, and regulatory clarity. A rigid AML framework poses the risk of holding back innovation, while overly flexible regulations could create loopholes for illicit activities.

Regulatory sandboxes and innovation hubs can serve as controlled environments where fintech firms test new AML solutions without facing immediate regulatory burdens. This fosters innovation while ensuring compliance mechanisms are effective before full-scale implementation (Rek, 2024; Rūse, 2014). International cooperation is also essential. Given the borderless nature of fintech transactions, AML enforcement cannot remain fragmented across jurisdictions, and a level playing field for fintech companies must be created (Koranteng & You, 2024). Policymakers should work toward a more harmonized global framework that supports innovation while ensuring robust AML enforcement; this could involve better cross-border collaboration between FIUs, standardized AML compliance requirements, and an increased role for global regulatory bodies in overseeing high-risk fintech activities. It could mean strengthening the role of the Financial Action Task Force (FATF), which sets international standards and provides recommendations on the prevention of global money laundering and terrorist financing. For example, the FATF could introduce real penalties for countries that fail to follow AML rules and work with global

organizations like the IMF and World Bank to apply economic pressure on non-compliant countries.

Finally, as underlined in a report by the European Institute of Innovation and Technology (2024), regulators and supervisors often lack the technological expertise needed to keep pace with rapid fintech innovation, making the implementation of even well-structured regulations difficult. To address this, supervisory bodies must upgrade their technological capabilities and make use of digital automated tools to strengthen oversight and enforcement in the evolving financial landscape.

Referring back to the original research question: AML laws impact the growth of fintech companies by burdening them with excessive compliance expenses which prevent them from using their resources to develop new products. AML regulations play a vital role in preserving financial market stability as well as maintaining investor and borrower trust within fintech platforms. The main challenge for regulators continues to be achieving proper equilibrium between the mentioned forces. This research contributes theoretically by underlining the need for a dynamic regulatory framework that combines principles of adaptive governance with financial innovation theory. It aims to conceptualize regulation as a system that evolves alongside innovation, strengthening the view that regulatory learning and technological adaptation must be a part of the same policy cycle. Such a framework can help reduce compliance costs for fintechs while preserving market integrity.

Future research should explore how emerging technologies (blockchain-based identity verification, AI-driven transaction monitoring, and cross-border data-sharing frameworks) can be put into practice within AML systems without comprising innovation or privacy. Empirical studies could also assess the effectiveness of regulatory sandboxes and innovation hubs across jurisdictions, identifying which governance structures best foster responsible innovation. Finally, future investigation could evaluate the long-term economic and social impacts of AML-driven compliance costs on the growth, competitiveness, and inclusivity of the fintech lending sector. The future development of fintech lending requires a united front which incorporates modern technology with worldwide, and standards and balanced regulatory measures to prevent money laundering and other financial criminal activities.[7]

7 ChatGPT, an AI language model developed by OpenAI, was utilized over a period of several weeks for paraphrasing and conducting grammar and syntax checks (OpenAI, personal communication, 16 March 2025 – 5 June 2025). The article was also copyedited by a human.

REFERENCES

Arner, D. W., Barberis, J., & Buckley, R. P. (2016). 150 years of fintech: An evolutionary analysis. *Jassa*, *3*, 22–29.

Arnone, M., & Borlini, L. (2010). International anti-money laundering programs. *Journal of Money Laundering Control*, *13*(3), 226–271. https://doi.org/10.1108/13685201011057136

Ayata, Z. (2024). European Union contracts in digital environments. In D. Ramiro Troitiño (Ed.), *E-governance in the European Union: Strategies, tools, and implementation* (pp. 173–185). Springer Nature Switzerland. https://doi.org/10.1007/978–3-031–56045-3_12

Baba, C., Batog, C., Flores, E., Gracia, B., Karpowicz, I., Kopyrski, P., Roaf, J., Shabunina, A., van Elkan, R., & Xu, X. C. (2020). *Fintech in Europe: Promises and threats* [IMF Working paper no. WP/20/24]. International Monetary Fund. https://doi.org/10.5089/9781513561165.001

Bartnik, K. (2025). Can a national financial supervisor support the development of the fintech sector? Innovation hubs as a tool for supporting innovation: The examples of Poland, Estonia, and Italy. *Białostockie Studia Prawnicze*, *30*(3), 215–230. https://doi.org/10.15290/bsp.2025.30.03.14

Berg, T., Fuster, A., & Puri, M. (2021). *Fintech lending* [NBER Working paper no. 29421]. National Bureau of Economic Research. https://doi.org/10.3386/w29421

Brummer, C., & Yadav, Y. (2017). The fintech trilemma. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.3054770

Buckley, R. P., Arner, D. W., Veidt, R., & Zetzsche, D. A. (2019). Building fintech ecosystems: Regulatory sandboxes, innovation hubs and beyond. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.3455872

Cambridge Centre for Alternative Finance. (2017). *Entrenching innovation: The 4th UK alternative finance industry report*. https://www.jbs.cam.ac.uk/wp-content/uploads/2020/08/2017–12-21-ccaf-entrenching-innov.pdf

Carney, M. (2017, 25 January). *The promise of fintech – something new under the sun?* [Speech] Deutsche Bundesbank G20 Conference on Digitising Finance, Financial Inclusion and Financial Literacy, Wiesbaden. https://www.bankofengland.co.uk/speech/2017/the-promise-of-fintech-something-new-under-the-sun

Committee on the Global Financial System & Financial Stability Board. (2017). *Fintech credit: Market structure, business models and financial stability implications*. https://www.fsb.org/uploads/CGFS-FSB-Report-on-Fintech-Credit.pdf

Cornelli, G., Frost, J., Gambacorta, L., Rau, P. R., Wardrop, R., & Ziegler, T. (2020). *Fintech and big tech credit: A new database* [BIS Working paper]. Bank for International Settlements. https://www.bis.org/publ/work887.htm

Costa, M. I. (2023). The legal concept of discrimination by association: Where does it fit into the digital era? *UNIO–EU Law Journal*, *9*(1), 16–28.

Council of the European Communities. (1991). Council Directive 91/308/EEC of 10 June 1991 on the Prevention of the Use of the Financial System for the Purpose of Money Laundering (O. J. L 166, 28.06.1991, pp. 77–83). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:31991L0308

European Banking Authority. (2025, July 28). *A careless use of innovative compliance products can lead to money laundering and terrorism financing risks, the EBA says in its opinion* [Press release]. https://www.eba.europa.eu/publications-and-media/press-releases/careless-use-innovative-compliance-products-can-lead-money-laundering-and-terrorism-financing-risks

European Commission. (2020). Communication from the Commission on an Action Plan for a Comprehensive Union Policy on Preventing Money Laundering and Terrorist Financing 2020/C 164/06 (Document 52020XC0513(03)). C/2020/2800. http://data.europa.eu/eli/dir/2024/1640/oj

European Institute of Innovation and Technology. (2024). *Fintech innovation: A balancing act between disruption and regulation* https://eit.europa.eu/library/fintech-innovation-balancing-act-between-disruption-and-regulation

European Securities and Markets Authority (ESMA). (2018). *Joint report on regulatory sandboxes and innovation hubs*. https://www.esma.europa.eu/sites/default/files/library/jc_2018_74_joint_report_on_regulatory_sandboxes_and_innovation_hubs.pdf

European Union. (2005). Directive 2005/60/EC of the European Parliament and of the Council of 26 October 2005 on the Prevention of the Use of the Financial System for the Purpose of Money Laundering and Terrorist Financing (O. J. L 309, 26.10.2005, pp. 15–36).

European Union. (2015). Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the Prevention of the Use of the Financial System for the Purposes of Money Laundering or Terrorist Financing (O. J. L 141, 20.05.2015, pp. 73–117).

European Union. (2023). Regulation (EU) 2023/1113 on Information Accompanying Transfers of Funds and Certain Crypto-Assets and Amending Directive (EU) 2015/849 (O. J. L 150, 09.06.2023, pp. 1–39).

European Union. (2024a). Regulation (EU) 2024/1620 of the European Parliament and of the Council of 31 May 2024 Establishing the Authority for Anti-Money Laundering and Countering the Financing of Terrorism (O. J. L 2024, 31.05.2024, pp. 45–60).

European Union. (2024b). Regulation (EU) 2024/1624 of the European Parliament and of the Council of 31 May 2024 on the Prevention of the Use of the Financial System for the Purposes of Money Laundering or Terrorist Financing (O. J. L 2024, 31.05.2024, pp. 1–30).

European Union. (2024c). Directive (EU) 2024/1640 of the European Parliament and of the Council of 31 May 2024 on the Mechanisms to Be Put in Place by Member States for the Prevention of the Use of the Financial System for the Purposes of Money Laundering or Terrorist Financing (O. J. L 2024, 31.05.2024, pp. 31–55).

Ferretti, F. (2022). A single European data space and data act for the digital single market: On datafication and the viability of a PSD2-like access regime for the platform economy. *Eur. J. Legal Stud.*, *14*, 173. https://dx.doi.org/10.2924/EJLS.2022.015

Giovanola, B. (2023). Justice, emotions, socially disruptive technologies. Critical Review of International Social and Political Philosophy, 26(1), 104–119. https://doi.org/10.1080/13698230.2021.1893255

Gopal, M., & Schnabl, P. (2022). The rise of finance companies and fintech lenders in small business lending. *Review of Financial Studies*, *35*(11), 4859–4901. https://doi.org/10.1093/rfs/hhac034

Hamuľák, O. (2016). *National sovereignty in the European Union: View from the Czech perspective*. Springer. https://doi.org/10.1007/978–3-319–45351-4

Kerikmäe, T.,Troitiño, D. & Shumilo, O. (2019). An Idol or an Ideal? A Case Study of Estonian E-Governance: Public Perceptions, Myths and Misbeliefs. Acta Baltica Historiae et Philosophiae Scientiarum. 7. 71–80. 10.11590/abhps.2019.1.05.

Koranteng, B., & You, K. (2024). Fintech and financial stability: Evidence from spatial analysis for 25 countries. *Journal of International Financial Markets Institutions and Money*, *93*, 102002. https://doi.org/10.1016/j.intfin.2024.102002

Kou, G., & Lu, Y. (2025). Fintech: A literature review of emerging financial technologies and applications. *Financial Innovation*, *11*(1). https://doi.org/10.1186/s40854–024-00668–6

Lagarde, C. (2018). *A regulatory approach to fintech*. Finance & Development. https://www.omfif.org/2018/09/a-regulatory-approach-to-fintech/

Langley, P., & Leyshon, A. (2020). The platform political economy of fintech: Reintermediation, consolidation and capitalisation. *New Political Economy*, *26*(3), 376–388. https://doi.org/10.1080/13563467.2020.1766432

Lentini, A., Munteanu, D. E., & Zennaro, F. (2025). *Fintech classification methodology* (Markets, Infrastructures and Payment Systems No. 61, pp. 1–40). Banca d'Italia. https://www.bancaditalia.it/pubblicazioni/mercati-infrastrutture-e-sistemi-di-pagamento/approfondimenti/2025–061/N.61-MISP_ENG.pdf?language_id=1

Maatsch, A. (2024). Parliamentary adjustment during a crisis: Interplay of digitalization and domestic context factors. *Internet of Things*, *27*, 101316. https://doi.org/10.1016/j.iot.2024.101316

Mazur, V., & Ramiro Troitiño, D. (2024). The members of the EU and e-governance, analysis, and institutional support. In D. Ramiro Troitiño (Ed.) *E-governance in the European Union: Strategies, tools, and implementation* (pp. 39–55). Springer Nature Switzerland. https://doi.org/10.1007/978–3-031–56045-3

Mokrá, L. (2023). Digitally sovereign individuals: The right to disconnect as a new challenge for European legislation in the context of building the EU digital market. In D. Ramiro Troitiño, T. Kerikmäe, & O. Hamuľák (Eds.) *Digital development of the European Union: An interdisciplinary perspective* (pp. 189–197). Springer International Publishing. https://doi.org/10.1007/978–3-031–27312-4_12

Omotoso, O. (2024). AML in cross-border fintech transactions: Risks and regulatory measures. *SSRN Working Paper*. https://doi.org/10.2139/ssrn.5038850

Outeda, C. C. (2024). The EU's AI Act: A framework for collaborative governance. *Internet of Things 27(3)*, 101291. https://doi.org/10.1016/j.iot.2024.101291

Rek, M. (2024). E-democracy in the EU. In D. Ramiro Troitiño (Ed.) *E-governance in the European Union: Strategies, tools, and implementation* (pp. 103–115). Springer Nature Switzerland. https://doi.org/10.1007/978–3-031–56045-3_8

Roide, N. (2022). Fintech and anti-money laundering regulation: Implementing an international regulatory hierarchy premised on financial innovation. *Texas A&M Law Review*, *9*(2), 465–496. https://doi.org/10.37419/lr.v9.i2.5

Rūse, I. (2014). Nordic–Baltic interaction in European Union negotiations: Taking advantage of institutionalized cooperation. *Journal of Baltic Studies*, *45*(2), 229–246. https://doi.org/10.1080/01629778.2013.846928

Suryono, R. R., Purwandari, B., & Budi, I. (2019). Peer to peer (P2P) lending problems and potential solutions: A systematic literature review. *Procedia Computer Science*, *161*, 204–214. https://doi.org/10.1016/j.procs.2019.11.116

Tomczak, T. (2025). Nadzór AML nad kryptoaktywami od 30.12.2024 r. – zmiany w Dyrektywie 2015/849 wprowadzone rozporządzeniem 2023/1113. *Białostockie Studia Prawnicze*, *30*(3), 125–138. https://doi.org/10.15290/bsp.2025.30.03.08

Troitiño, D. R. (2023). EU elections and internet voting (i-voting). In D. Ramiro Troitiño, T. Kerikmäe, & O. Hamuľák (Eds.) *Digital development of the European Union: An interdisciplinary perspective* (pp. 319–333). Springer International Publishing. https://doi.org/10.1007/978–3-031–27312-4_20

Wang, Y. (2023). The impact of financial technology development on money laundering risks. In A. Bhunia, R. B. Ahmad, & Y. Zhu (Eds.), Advances in economics, business and management research (pp. 180–192). https://doi.org/10.2991/978–94-6463–298-9_20

Wangchuk, P. (2021). Common types of crowdfunding models, related concepts and its impact on business: A brief literature review. *Asian Journal of Economics Business and Accounting*, 56–63. https://doi.org/10.9734/ajeba/2021/v21i1430471

Wójcik, D. (2020). Financial geography I: Exploring fintech – maps and concepts. *Progress in Human Geography*, *45*(3), 566–576. https://doi.org/10.1177/0309132520952865

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

sciendo

DOI: 10.15290/bsp.2026.31.01.14

Received: 07.08.2025
Accepted: 16.10.2025

Paweł Czaplicki
University of Bialystok, Poland
p.czaplicki@uwb.edu.pl
ORCID ID: 0000–0002–9782–7252

E-Voting in Commercial Companies in Poland from the Perspective of Shareholders as an Example of Digital Democracy: Challenges and Opportunities

Abstract: This article addresses the issue of e-voting in commercial companies in Poland from the perspective of the company's shareholders. It presents this issue as an example of digital democracy and discusses the associated challenges and opportunities. The article is based on the dogmatic-legal and the comparative-legal methods. The main aim is to examine whether regulations regarding e-voting by shareholders on the resolutions of commercial companies in Poland have improved the conduct of shareholder voting or have established barriers that complicate this process. The second research issue is an attempt to answer the question of whether regulations introduced by the Polish legislature enable the use of modern technologies for conducting voting, including systems based on distributed ledger technology and virtual worlds. The research allowed for the formulation of the following research theses: firstly, the regulations contained in the Polish Commercial Companies Code allow for the widespread use of electronic voting methods by shareholders when resolutions are adopted. However, they are not available in all commercial companies, nor to the same extent. Secondly, voting using methods based on distributed ledger technology is also permissible. However, voting at a meeting cannot be conducted solely virtually. The conclusions include proposals for clarification of the legal provisions in this area, which will enable more effective use of e-voting in commercial companies in Poland.

Keywords: commercial companies, digital democracy, distributed ledger technology, e-voting, virtual worlds

Introduction

The legal regulations regarding e-voting by shareholders on the resolutions of commercial companies in Poland were recently amended in the Commercial Companies Code by the Act of 31 March 2020 Amending the Act on Special Solutions Related to the Prevention, Counteraction, and Combating of COVID-19, Other Infectious Diseases and the Resulting Crisis Situations, and Certain Other Acts.[1] These amendments were dictated by the need to enable company meetings and voting to be held electronically due to the COVID-19 pandemic. Unfortunately, the legislation has not treated all the provisions of the Commercial Companies Code uniformly. In some companies, the possibility of using e-voting during the adoption of resolutions by shareholders is the rule; in others it is an exception that must be provided for in the articles of association, and in others, such a possibility has not been foreseen at all. This raises a fundamental question about the advisability of differentiating commercial companies in this regard. It also requires an examination of whether the regulations regarding e-voting by shareholders on resolutions in commercial companies in Poland have improved the conduct of shareholder voting or have established barriers that have complicated the process.

In the context of e-voting, it is also reasonable to ask about the possibility of using modern technologies during e-voting, including systems based on distributed ledger technology and virtual worlds. The legislature did not explicitly provide for such a solution in the regulations, but on the other hand, it did not impose any restrictions in this regard. Therefore a fundamental question arises: do the regulations introduced by the Polish legislature not in practice hinder the use of the modern technologies mentioned above for conducting voting?

An analysis of the content of these national regulations, presented in detail below, allows for the formulation of two basic research hypotheses. Firstly, the regulations contained in the Polish Commercial Companies Code allow for the widespread use of e-voting methods by shareholders. However, they are not available in all commercial companies, nor to the same extent. Secondly, voting using methods based on distributed ledger technology is also permissible. However, holding a virtual meeting is not possible. Consideration should also be given to whether there is a need to clarify the legal provisions in this area, which would allow for more effective use of e-voting in commercial companies in Poland.

1 For information on the previously existing rules for the use of e-voting in commercial law companies in Poland, see Kappes, 2009; Krukowska-Korombel, 2010; Oplustil, 2008; Romanowski & Opalski, 2009; Żaba, 2020.

1. Models of e-voting in commercial companies in Poland

Legal regulations related to e-voting currently cover three types of capital companies, i.e. limited liability companies, simple joint-stock companies, and joint-stock companies. In a limited liability company, Article 234(1) of the Commercial Companies Code stipulates that participation in a shareholders' meeting may also be undertaken using electronic means of communication, unless the articles of association provide otherwise. This regulation should be assessed positively, as it establishes the possibility of conducting electronic shareholders' meetings as a rule. The provision also clarifies the scope of shareholders' rights related to participation in an electronic shareholders' meeting: participation in such a meeting includes, among other things, exercising the right to vote in person or through a proxy before or during the meeting. This solution should also be assessed positively. The literature rightly points out that enabling shareholders not only to participate in the shareholders' meeting but also to vote electronically allows them to effectively exercise their corporate rights (Lewandowski, 2020, p. 769). It should also be noted that detailed rules for participating in shareholders' meetings using electronic means of communication are defined in the by-laws; this principle is also positive. Specifying the tools for voting at shareholders' meetings in a legal provision or the articles of association could pose a barrier if new technologies emerge that the legislature was unable to anticipate at the time of drafting the regulations; in such a situation, new technologies would be excluded. It is significantly easier to amend by-laws than statutes or articles of association. Importantly, by-laws cannot specify requirements and restrictions that are not necessary to identify shareholders and ensure the security of electronic communications. This approach by the legislature should also be appreciated. The provision clearly limits the possibility of introducing any restrictions on the exercise of corporate rights to vote at a shareholders' meeting to a minimum. The company must be able to verify whether the person entitled to do so is actually participating and voting. In other respects, the company and its shareholders are free to determine the technical conditions for participation in shareholders' meetings. Furthermore, pursuant to Article 238 § 3 of the Commercial Companies Code, if participation in a shareholders' meeting takes place using electronic means of communication, the notification must also include information, among other things, on the manner of exercising voting rights. Information in this scope is indeed essential, as shareholders must be able to prepare for voting at the meeting, including from a technical perspective. Under Article 248 § 2 of the Commercial Companies Code, the minutes of the meeting must include, among other things, a list of the shareholders voting electronically; in such a situation, the signatures of the participants are not required. The above provision should be assessed as rational: since a shareholder participates in the meeting and votes electronically, they cannot be required to physically sign documents prepared during the meeting.

In the case of a simple joint-stock company, the legislation has guaranteed shareholders even broader opportunities to use e-voting during the adoption of resolutions. Pursuant to Article 300(80) of the Commercial Companies Code, shareholder resolutions are adopted at a general meeting, or outside a general meeting in writing or using electronic means of communication. The difference compared to a limited liability company is that in this company, the ability to adopt resolutions using electronic means of communication exists only within the framework of the shareholders' meeting. The literature clearly indicates that exercising voting rights in a limited liability company using electronic means of communication always implies the need to hold a shareholders' meeting (Żaba, 2020, p. 17). In a simple joint-stock company, shareholders also have this option outside the general meeting. However, it should be emphasized that shareholders may vote using electronic means of communication if these are specified in the company's articles of association or if all shareholders have expressed their consent to such voting in writing. The aforementioned stipulation therefore requires the authors of the company's articles of association to specify methods for voting on electronic resolutions at the stage of concluding the articles. An alternative to regulating this issue in the articles of association is the consent of all shareholders at the stage of adopting a specific resolution. The legislation does not mandate the use of additional measures to ensure the correct casting of a vote by an authorized person, such as a qualified electronic signature, trusted profile, or other security measures that will ensure the vote's validity.

Considering the aforementioned definition of 'electronic means of communication', which assigns primary status, through the phrase 'in particular', to email, it should be noted that the correct casting of a vote using this means may pose the greatest controversy. The absence of these additional safeguards may allow for greater latitude for an unauthorized person to cast a vote, which in turn may result in the adoption of a resolution that is flawed (Kawalec, 2021, p. 4). It is also worth noting that, pursuant to Article 300(100) § 4 of the Commercial Companies Code, resolutions adopted in writing pursuant to Article 300(80) are entered by the management board in the minutes book. Resolutions adopted using electronic means of communication are attached to the minutes book in the form of printouts of the resolutions, certified by the signature of a management board member. This simplification of procedures should be viewed positively. As resolutions adopted electronically cannot be signed with traditional signatures due to technical barriers, certification of the resolution's content by a management board member should be considered sufficient in this case.

The issue of participation and voting in the general meeting of a simple joint-stock company using electronic means of communication is also different. As Article 300(92) of the Commercial Companies Code provides, in the case of a simple joint-stock company, the articles of association may permit participation in the general meeting using electronic means of communication. Therefore the regulations do not automatically provide for such a possibility; the problem related to this specific

inconsistency in the legislation has already been highlighted in the literature (Szczepańska & Ryszkowski, 2025, pp. 44–46; Szumański, 2020, p. 5). Therefore the option to vote at the general meeting electronically must be established by the company's shareholders in the articles of association. If the articles of association provide for the possibility of holding an electronic general meeting, this right must also include the exercise of voting rights in person or by proxy before or during the meeting. In this respect, the solution provided by the legislation is analogous to a limited liability company. The doctrine emphasizes that, taking into account the rapid development of technology, the legislation has refrained from describing detailed technical conditions for participation in the general meeting using electronic means of communication, entrusting these issues to the companies themselves (Dumkiewicz, 2025, p. 1). Moreover, shareholder participation in the general meeting may only be subject to the requirements and restrictions necessary to identify shareholders and ensure the security of electronic communications. The articles of association cannot provide for additional restrictions that would constitute a barrier to shareholder participation and voting at the general meeting of a simple joint-stock company. The comments made in this regard with respect to a limited liability company also apply to a simple joint-stock company. Detailed rules regarding participation in the general meeting using electronic means of communication are set out in the general meeting regulations. Article 300(100) § 1 of the Commercial Companies Code further specifies that a list of shareholders voting using electronic means of communication shall be attached to the minutes of the general meeting. The comments made with respect to a limited liability company also apply to a simple joint-stock company in this issue.

The regulations regarding e-voting by shareholders on resolutions are most extensive in joint-stock companies. This is due, among other things, to the fact that joint-stock companies come in two forms: private and public.[2] Firstly, it should be noted that, pursuant to Article 406(5) of the Commercial Companies Code, participation in a general meeting may also take place using electronic means of communication, unless the statutes provide otherwise. Participation in an electronic general meeting includes, among other things, the ability to exercise voting rights in person or through a proxy before or during the meeting. As the literature rightly points out, this is the most comprehensive way to participate in a general meeting using electronic means of communication. It is also rightly noted that this creates the problem of identifying the person casting the vote (Pabis, 2016, p. 16); in this regard, the company should implement a voting technique that ensures security. The supervisory board is responsible for defining in separate regulations detailed rules for participating in a general meeting using electronic means of communication. The regulations may not specify require-

2 A public company is a company with at least one share admitted to trading on a regulated market or introduced to trading in an alternative trading system in the territory of the Republic of Poland, i.e. a company listed on the stock exchange.

ments or limitations that are not necessary to identify shareholders and ensure the security of electronic communication. It is rightly emphasized in the legal literature that the provisions of Article 406(5) of the Commercial Companies Code do not refer in any way to the location (place) of persons participating in a general meeting via electronic means of communication, including those casting their votes electronically. This means that they may be present in any location (town) in any country, and this will not violate the provisions of the Commercial Companies Code regarding the necessity of holding a general meeting in the territory of the Republic of Poland (Leśniak, 2020, pp. 23–24). Furthermore, pursuant to Article 421 § 2 of the Commercial Companies Code, a list of shareholders voting using electronic means of communication is attached to the minutes of the general meeting. The regulations concerning joint-stock companies, mentioned above, are therefore analogous to those provided for in limited liability companies. The comments made in the above-mentioned areas of electronic voting at shareholders' meetings of limited liability companies will therefore also apply to voting at general meetings of joint-stock companies.

However, the new obligation that the legislature has introduced for joint-stock companies is that if voting rights are exercised using electronic means of communication, the company must immediately send the shareholder an electronic confirmation of receipt of the vote (Article 406(5) § 5 of the Commercial Companies Code). Additionally, with respect to public joint-stock companies, the legislature has decided that the announcement of a general meeting of a public company should include, among other things, information on the method of exercising voting rights by using electronic means of communication (Article 402(2) of the Commercial Companies Code).

In the context of the regulations analysed above, the lack of regulation regarding the use of electronic communication means in adopting resolutions by partners in partnerships is striking. In this regard, the legislature has included basic regulations in the Commercial Companies Code, primarily with respect to general partnerships. Only relevant clarifications have also been included in the provisions governing professional partnerships, limited partnerships, and limited joint-stock partnerships. First of all, it is worth noting that, pursuant to Article 43 of the Commercial Companies Code, which pertains to a general partnership, in matters exceeding the scope of the partnership's ordinary activities, the consent of all partners is required, including those excluded from managing the partnership's affairs. The provision does not specify how and in what form the partners' consent should be expressed. Serious doubts have been raised as to whether a decision by partners in a matter exceeding the scope of ordinary activities should necessarily take the form of a resolution (Rodzynkiewicz, 2013, p. 99). Furthermore, the literature indicates that since the legislation does not specify the rules for expressing consent to handle matters exceeding the scope of ordinary activities, it should be assumed that the partners' consent may be expressed in writing or in another clear and unambiguous manner (Borowy, 2024, p. 251). Therefore it should be assumed that voting via electronic means of communication is also permissible in

a general partnership, based on the principle of freedom of choice regarding the form of decision-making. However, under current law, it seems justified to recommend that partners of general partnerships should clarify the technical aspects of decision-making in their partnership agreement. This will prevent conflicts between partners over this matter during the partnership's commercial operation.

In the context of other partnerships, it should be noted that in the case of a professional partnership, the legislation has not provided for separate rules for partners' decision-making. Therefore, pursuant to Article 89 of the Commercial Companies Code, the rules for a general partnership apply. The comments above therefore remain relevant in the context of a professional partnership. In the case of a limited partnership, pursuant to Article 121 § 2 of the Commercial Companies Code, the consent of the limited partner is required for matters beyond the scope of the partnership's ordinary activities, unless the partnership agreement provides otherwise. This means that all the partners – both general and limited – participate in making the main decisions for the partnership. In this case, the legislation has not provided for detailed rules for partners' voting; therefore similar requirements can be formulated for a limited partnership as for a general partnership.

The final type of partnership is the limited joint-stock partnership. In the case of this company, the legislation has not provided specific rules for conducting voting when decisions are made by general partners and shareholders. At the same time, Article 126 § 1 established the principle that in matters not regulated by the general partners' regulations, the provisions of the general partnership shall apply, while the provisions of a joint-stock company shall apply to shareholders and their participation in the general meeting. In the case of a limited joint-stock partnership, the regulation of voting in decision-making is therefore complex. With respect to votes involving general partners, the legislation has not explicitly provided for the possibility of voting using electronic means of communication, so the comments made regarding the voting process on resolutions in a general partnership will be relevant. However, in the case of votes conducted at a general meeting involving shareholders, the regulations for a joint-stock company shall apply. Therefore, as already presented above, voting via electronic means of communication has been provided for by the legislation and is thus entirely possible. The example of a limited joint-stock partnership is an excellent summary of how inconsistent the legislation is in the case of e-voting rules in commercial companies in Poland.

2. Voting by shareholders of commercial companies on resolutions through the use of modern technologies

A positive aspect of the current shape of the regulations governing voting on resolutions in companies is the technological neutrality emphasized in the doctrine

(Szumański, 2020, p. 10). The regulations' lack of clarification regarding the technical aspects of voting allows for the use of various solutions, including modern technologies. It will also not constitute a limitation in the event of the appearance of new methods and techniques for conducting virtual voting, which the legislature could not have foreseen and taken into account before. Considering the above arguments, it should be stated that under Polish law, there are no obstacles to using systems based on distributed ledger technology to conduct votes on resolutions, particularly in commercial companies.

The literature has long suggested that distributed ledger technology could also be used in the voting process of shareholders in commercial companies (Bilski & Kiełbus, 2024, p. 77). An excellent example of blockchain technology in this regard is the e-voting application offered by the National Depository for Securities (KDPW) (KDPW, 2023). E-voting is the KDPW's application for remote participation and voting at company general meetings. According to information it has provided, the application is a modern, secure, and inexpensive tool that enables active participation in general meetings from anywhere and at any time, facilitates access to reliable information about general meetings, and provides consistent, transparent, and undeniable insight into the results of the meeting, including investors' voting patterns. It should also be emphasized that thanks to the use of blockchain technology, the organization and management of general meetings of shareholders can be transferred to a fully digital dimension while simultaneously meeting statutory requirements regarding the identification of shareholders and ensuring the security of electronic communication.

The main disadvantage of this tool is that the KDPW offers it only to companies whose shares are registered with them; therefore only joint-stock companies can use it. It is not available to other commercial companies, particularly limited liability companies and simple joint-stock companies, where it could find a practical application. Another inconvenience of the application is that it requires an additional fee; therefore joint-stock companies wishing to use modern blockchain technology for voting at general meetings must expect additional costs. In this context, it would be advisable to develop and provide a dedicated electronic voting tool for all commercial companies. The Ministry of Digital Affairs, in collaboration with the Ministry of Finance and Economy, could undertake this task. The creation of such a tool would allow Polish commercial companies to enter a new era of technological development, which could contribute to more efficient management in the future. This in turn could lead to improvement in the financial results of commercial companies in Poland.

The second significant challenge for the Polish legislature is the issue of the shareholders of commercial law companies conducting votes on resolutions in virtual meetings. In this context, it should be noted that while there are no obstacles to using distributed ledger technology in the e-voting process in commercial companies in Poland, the literature rightly points out that the provisions of the Commercial

Companies Code in its current shape exclude the possibility of holding and voting at a company's general meeting in cyberspace, i.e. without designating a physical location for the meeting (Szumański, 2020, p. 10). Each type of company has a provision requiring the meeting to be held in a real location, by definition at the company's registered office (Articles 234, 300(88), and 403 of the Commercial Companies Code). As rightly emphasized in the literature, the term 'place' used by the legislation in the above-mentioned provisions means 'a limited section of space in the geographical sense', but does not include the possibility of choosing a virtual space (a so-called place on the network) (Engeleit, 2005, pp. 232–236). However, one cannot agree with the view that the regulation regarding the place for a shareholders' meeting of a 'traditional' limited liability company and the place for a general meeting of a joint-stock company differs from the regulation contained in Article 240(1) § 1 and 2 of the Commercial Companies Code regarding the adoption of resolutions by shareholders in a so-called e-limited liability company. The latter provisions are a source of norms that do not require an unambiguous determination of the place (location) for a shareholders' meeting of the e-limited liability company (Leśniak, 2020, p. 23). It should be noted that Article 240(1) of the Commercial Companies Code applies to adopting resolutions electronically, but only outside of a shareholders' meeting. Therefore equating this situation with the possibility of holding a virtual shareholders' meeting in an e-limited liability company is not justified.

In this context, it should also be noted that the laws of other countries already provide for the possibility of shareholders of commercial companies adopting resolutions during virtual meetings. A prime example is the Austrian Virtual Meetings Act (VirtGesG) (Nationalrat Österreich, 2023; Parlament Österreich, 2023), which allows for virtual or hybrid shareholder meetings and general meetings for commercial companies. While virtual meetings in Austria were temporarily permitted during the COVID-19 pandemic, the VirtGesG creates a permanent framework for such meetings, allowing for exclusive virtual or hybrid participation. However, it should be noted that fully virtual general meetings are only permitted in those companies where such a possibility is provided for in the articles of association or statute. It should also be emphasized that the VirtGesG does not cover the meetings of internal corporate bodies, such as executive or supervisory boards, where a different legal situation applies. In terms of the basic assumptions for conducting virtual meetings, it should be noted that the law requires that the technology used for virtual meetings ensures participants can exercise their rights effectively, including the right to vote. This means, among other things, that participants must be provided with an acoustic and optical two-way connection in real time. The articles of association can specify whether the virtual meeting is to be held as a 'simple' or a 'moderated' general meeting. Whereas in the standard case of a simple virtual meeting there is a two-way connection, i.e. all participants can speak at any time, in a moderated virtual general meeting, the meeting is primarily broadcast, but with the possibility of written com-

munication at any time (e.g. by chat, email, or in a separate portal) and, at the request of a participant or if the chairperson of the meeting gives a participant the floor, also through oral contributions or questions. The software to be used and other technical requirements may be specified in the articles of association or (at the latest) determined and communicated by the chair at the time of the invitation. However, virtual participation must be possible easily and free of charge, without having to download any specific software. It is also important to point out that the provisions in the articles of association allowing for virtual and/or hybrid meetings must be limited to a maximum of five years. However, a resolution on the extension of the period of validity may be passed by way of a virtual or hybrid general meeting (Aichhorn-Wöss & Maras, 2024; Cerha Hempel, 2023; Heffermann & Lechner, 2023; Trondl, 2023).

Returning to the regulations of Polish law: holding company meetings in a different format, e.g. using platforms supporting virtual worlds or the metaverse, is currently not possible. It is worth considering whether conducting voting in this type of condition would be permissible in partnerships. As indicated above, no provision specifies the form of decision-making in partnerships, so the right to use virtual worlds for this purpose could be derived from the fundamental principle of private law that what is not prohibited is permitted. On the other hand, transferring real decision-making in current matters to virtual worlds without a clear legal basis could be considered far-reaching. Therefore, under the current legal framework, it should be assumed that voting on resolutions in commercial companies using virtual worlds is not possible. This does not change the fact that in a world where we are observing such dynamic technological progress, the legislature's reference to the concept presented above will soon pose another legislative challenge. Actions in this direction are already being taken at the European Union level.[3]

Conclusions

To summarize the models of e-voting in commercial companies in Poland: it should be noted that the lack of a clear indication of the possibility of conducting e-voting in partnerships is striking. Secondly, the legislation's inconsistency is striking: for limited liability companies and joint-stock companies, e-voting is a rule, while for simple joint-stock companies, this option is allowed only as an exception, which must be reflected in the articles of association. Conversely, in the case of simple joint-stock companies, the legislation also allows for the adoption of resolutions outside the general meeting through using electronic means of communication, while in limited liability

3 In this context, it is worth noting the European Commission's strategy on Web 4.0 and virtual worlds. The initiative aims to drive the next technological transformation and ensure an open, secure, trustworthy, fair, and inclusive digital environment for EU citizens, businesses, and public administrations (ec.europa.eu).

companies, this solution is limited solely to votes conducted during a shareholders' meeting. Thirdly, the legislation only obligates the company to send a confirmation of the vote to the voting shareholder in the case of joint-stock companies.

It therefore seems necessary to clarify the provisions of the Commercial Companies Code in the following areas. Firstly, to eliminate any doubts, the legislature should clarify the wording of Articles 43 and 121 § 2 of the Commercial Companies Code, clearly specifying that consent may also be expressed via electronic means of communication. At the same time, it should be noted that the detailed rules for shareholders' participation in voting via electronic means should be specified in the regulations adopted by the shareholders. Implementing this change will clarify the rules for electronic voting in all commercial companies; this will be achieved because Article 43 of the Commercial Companies Code will also resolve this issue for partners in a professional partnership as well as general partners in limited partnerships and limited joint-stock partnerships, to which it will apply accordingly.

Secondly, it is recommended that Article 300(92) of the Commercial Companies Code is amended and that the principle that participation in a general meeting may also be taken using electronic means of communication, unless the articles of association provide otherwise, is adopted. This postulate has already been formulated in the literature and deserves full support (Szczepańska & Ryszkowski, 2025, p. 49). Conversely, it seems reasonable to amend Article 227 of the Commercial Companies Code by adding a second sentence to § 2, reading 'Resolutions may also be adopted using electronic means of communication without holding a shareholders' meeting', and § 3, which would specify that shareholders may vote using electronic means of communication if these are indicated in the articles of association or if all shareholders have expressed written consent to such voting.

Thirdly, to ensure security and certainty of voting, it would be necessary to introduce into the regulations of limited liability companies and simple joint-stock companies an equivalent of Article 406(5) § 5 of the Commercial Companies Code, according to which, if voting rights are exercised using electronic means of communication, the company must immediately send the shareholder an electronic confirmation of receipt of the vote. The legislature could adopt these principles, for example, by adding Article 234(1) § 2(2) and Article 300(92) § 1(1) of the Commercial Companies Code, respectively.

Regarding the possibility of using modern technologies to vote on the resolutions of commercial companies in Poland, it should be concluded that under Polish law, there are no obstacles to using systems based on distributed ledger technology for this purpose, especially in commercial companies. However, in this context, it seems justified to create a common, uniform e-voting platform based on blockchain technology, accessible to all commercial companies. On the other hand, due to the need to hold meetings in a physical location, virtual worlds cannot be used to conduct electronic voting in companies. However, this possibility should not be under-

estimated, because with technological advances and the growing popularity of such platforms, the Polish legislature will soon face the challenge of regulating this issue. The first step in this direction should be the adoption of regulations similar to those provided for in Austrian law, which would enable the holding of shareholders' meetings and general meetings without a need to indicate the physical place where they are to be held. This stage, after adapting other legal provisions to the needs of conducting virtual meetings, including those concerning notary participation in meetings, is already achievable. Moving meetings to entirely virtual worlds is a long way off, but we should be thinking about it now.

The above considerations, both in relation to current legal provisions and the future challenges awaiting the Polish legislature and participants in commercial companies, demonstrate that these are excellent grounds for developing the idea of digital democracy.

REFERENCES

Aichhorn-Wöss, S., & Maras, C. (2024, 1 February). *Virtual shareholder meetings: New legal basis and requirements*. https://www.schoenherr.eu/content/virtual-shareholder-meetings-new-legal-basis-and-requirements

Bilski, A., & Kiełbus, R. (2024). *Kryptoaktywa i blockchain. Technologia, prawo, biznes*. Wolters Kluwer.

Borowy, B. (2024). Komentarz do art. 43 Kodeksu spółek handlowych. In Z. Jara (Ed.), *Kodeks spółek handlowych. Komentarz* (pp. 250–252). C. H. Beck.

Cerha Hempel. (2023, 2 June). *Virtual meetings – Austrian Act on Virtual Meetings*. https://www.cerhahempel.com/blog/start-ups-venture-capital-and-private-equity/virtual-meetings-austrian-act-on-virtual-meetings

Dumkiewicz, M. (2025). Komentarz do art. 300[92] Kodeksu spółek handlowych. In M. Dumkiewicz & A. Kidyba (Eds.), *Komentarz aktualizowany do art. 1–300 Kodeksu spółek handlowych* (pp. 1–2). Wolters Kluwer Polska.

Engeleit, M. (2005). *Wirtualne walne zgromadzenie. Wpływ internetu na prawo spółki akcyjnej*. Difin.

European Commission. (2024, July 30). *Światy wirtualne*. https://digital-strategy.ec.europa.eu/pl/factpages/virtual-worlds

Heffermann, V., & Lechner, I. (2023). *Virtual Shareholder Meetings Act (Virtuelle Gesellschafterversammlungen-Gesetz – VirtGesG): Creation of a permanent legal basis for virtual and hybrid meetings*. https://steuernachrichten.pwc.at/en/blog/2023/07/12/virtual-shareholder-meetings-act-virtuelle-gesellschafterversammlungen-gesetz-virtgesg-creation-of-a-permanent-legal-basis-for-virtual-and-hybrid-meetings/

Kappes, A. (2009). Elektroniczne głosowania na walnych zgromadzeniach akcjonariuszy. *Przegląd Prawa Handlowego*, *6*, 11–15.

Kawalec, G. A. (2021). Komentarz do art. 300[80] Kodeksu spółek handlowych. In R. Adamus & P. Malinowski (Eds.), *Prosta spółka akcyjna. Komentarz* (pp. 1–5). Wolters Kluwer Polska.

KDPW (National Depository for Securities). (2023). *eVoting – elektroniczne głosowanie na walnych zgromadzeniach*. https://www.kdpw.pl/pl/evoting.html

Krukowska-Korombel, J. (2010). Prawa akcjonariuszy wykonywane za pośrednictwem środków elektronicznych w świetle przepisów kodeksu spółek handlowych. *Przegląd Prawa Handlowego*, *9*, 36–43.

Leśniak, M. (2020). Udział w zgromadzeniu spółki kapitałowej za pomocą środków komunikacji elektronicznej po zmianach Kodeksu spółek handlowych dokonanych w ramach tzw. tarczy antykryzysowej. *Prawo Mediów Elektronicznych*, *2*, 20–24.

Lewandowski, P. (2020). Konsekwencje wadliwego zwołania elektronicznego zgromadzenia wspólników spółki z ograniczoną odpowiedzialnością. In M. Dumkiewicz, K. Kopaczyńska-Piczniak, & J. Szczotka (Eds.), *Sto lat polskiego prawa handlowego. Księga jubileuszowa dedykowana Profesorowi Andrzejowi Kidybie. Tom I* (pp. 767–780). Wolters Kluwer.

Nationalrat Österreich. (2023). Bundesgesetz über die Durchführung virtueller Gesellschafterversammlungen (VirtGesG), BGBl I 2023/79.

Oplustil, K. (2008). Dyrektywa 2007/36/WE w sprawie wykonywania niektórych praw akcjonariuszy i jej wpływ na prawo polskie – cz. II. *Monitor Prawniczy*, *3*, 119–125.

Pabis, R. (2016). Komentarz do art. 406[5] Kodeksu spółek handlowych. In A. Opalski (Ed.), *Kodeks spółek handlowych. Tom IIIB. Spółka akcyjna. Komentarz. Art. 393–490* (pp. 1–27). C. H. Beck.

Parlament Österreich. (2023). *Virtuelle Gesellschafterversammlungen-Gesetz Ministerialentwurf Erläuterungen 271/ME XXVII. GP*. https://www.parlament.gv.at/dokument/XXVII/ME/271/fname_1555993.pdf

Rodzynkiewicz, M. (2013). *Kodeks spółek handlowych. Komentarz*. Lexis Nexis.

Romanowski, M., & Opalski, A. (2009). Nowelizacja Kodeksu spółek handlowych w sprawie wykonywania niektórych praw akcjonariuszy spółek notowanych na rynku regulowanym. *Monitor Prawniczy*, *7*(supplement), 1–20.

Sejm of the Republic of Poland. (2000). Act of 15 September 2000, Commercial Companies Code (consolidated text of 2024, item 18, as amended).

Sejm of the Republic of Poland. (2023). Act of 31 March 2020 Amending the Act on Special Solutions Related to the Prevention, Counteraction, and Combating of COVID-19, Other Infectious Diseases and the Resulting Crisis Situations, and Certain Other Acts (Dz.U. 2020, item 568, as amended).

Szczepańska, K., & Ryszkowski, K. (2025). Problem adekwatności rozwiązań prawnych przyjętych przez polskiego ustawodawcę dla zgromadzeń online wspólników spółek kapitałowych – ze szczególnym uwzględnieniem regulacji dotyczących prostej spółki akcyjnej. *Białostockie Studia Prawnicze*, *30*(3), 37–55.

Szumański, A. (2020). Nowa regulacja udziału w zgromadzeniu spółki kapitałowej przy wykorzystaniu środków komunikacji elektronicznej. *Przegląd Prawa Handlowego*, *5*, 4–14.

Trondl, L. (2023, 21 September). *Austria: Virtual meetings at corporations, cooperatives, associations, mutual insurance associations, small insurance associations and savings banks ('companies') are permanently possible*. https://www.warwicklegal.com/news/666/austria-virtual-meetings-at-corporations-cooperatives-associations-mutual-insurance-associations-small-insurance-associations-and-savings-banks-companies-are-permanently-possible

Żaba, M. (2020). Uczestnictwo i głosowanie na zgromadzeniu wspólników przy wykorzystaniu środków komunikacji na odległość. *Przegląd Ustawodawstwa Gospodarczego*, *3*(861), 13–20.

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

sciendo

DOI: 10.15290/bsp.2026.31.01.15

Received: 21.06.2025
Accepted: 13.12.2025

Maria Marczewska-Rytko
Maria Curie-Skłodowska University, Lublin, Poland
m_marczewska@yahoo.com
ORCID ID: 0000–0002–4006–0476

Electronic Communication Tools in Participatory/Civic Budgeting: The Case of Warsaw[1]

Abstract: The aim of this study is to analyse the participatory/civic budget in Warsaw in terms of the use of electronic communication tools. Answers to the following two research questions are sought: (1) At what stages of participatory/civic budgeting are electronic tools used? (2) What are residents' opinions regarding electronic tools used in participatory/civic budgeting in Warsaw? During the research process, the following research hypothesis will be verified: the electronic tools used in the participatory/civic budget in Warsaw are being gradually improved, and the budget in this city is increasingly becoming an electronic one. This research primarily uses an in-depth analysis of primary sources, including statistical data, legal acts, reports, and evaluation documents. Eleven versions of the participatory/civic budget in Warsaw were analysed. The research hypothesis was partially verified positively.
Keywords: civic budget, participatory budget, Warsaw, electronic communication tools

Introduction

Participatory budgeting is a form of social consultation (with results that are binding on the government), which is one of the tools of participatory democracy and public co-management (Bateman, 2020; Lerner, 2014; Marczewska-Rytko &

1 The article presents some of the research results obtained during the research project "The Comparative Analysis of French and Polish Participatory Budgeting" at the Paris-Est Créteil University val de Marne, Centre d'Étude des Discours, Images, Texts Écrits, Communication (Céditec) in Paris from 1 May to 15 June 2025 and at Catholic University of Lille in Lille from 15 to 30 June 2025. The project was made possible thanks to a scholarship from the French Government.

Maj, 2021; Sintomer et al., 2016; Wampler et al., 2021; Zawadzka-Pąk & Tomáškova, 2019). In practice, the institution of participatory budgeting combines, to varying degrees, elements of both direct and deliberative democracy, depending on the country in which it is used (Marczewska-Rytko, 2024a). In Poland, the literature on the subject and in social and political practice uses two terms: 'civic budgets' and 'participatory budgets' (Sroka et al., 2022). The use of the concept of a civic budget is supported by the fact that in this case, the emphasis is transferred from participation as a specific activity to the entity performing this activity, that is, the citizens. Some researchers, however, point out that participatory budgeting is not limited to citizens, and that people who are not citizens of a given country can take part in the decision-making process (Kębłowski, 2013, p. 8). Some authors use the term 'civic/participatory budget' (Marczewska-Rytko, 2024b). Outside Poland, the term participatory budget is most often used. In Warsaw, the Polish capital, the initial name of participatory budget was changed to civic budget. Due to the complexity of the problem and the diverse practices in the research that has been conducted, the term participatory budget is used in relation to the first five versions of budgets in Warsaw, and civic budget in relation to the other versions.

In the era of an information society and the increasing use of electronic tools in our everyday lives, it is important to analyse the functioning of participatory/civic budgets from the perspective of e-democracy and e-participation. An important element is electronic voting (e-voting), which is defined as voting using electronic devices. Electronic participation refers to the inclusion (e-engagement) of citizens in public affairs through electronic communication, including electronic consultations (e-consultations). This is particularly important when citizens feel that they are not represented by their elected officials and doubt the effectiveness of participation as a tool for solving public problems (Allegretti, 2014). Therefore high hopes are placed on the use of modern information and communication technologies to increase public participation in the decision-making process (Friess, 2021). For example, modern communication tools allow citizens to digitally access information (Troitiño, 2022); they can also amplify citizens' voices and improve the quality of public services, but only if the technology is properly designed and linked to real, useful institutional, political, and social pathways. For example, the issue of access inequality has been highlighted, as these tools can amplify the voices of those with access and digital skills (Peixoto & Fox, 2016). It should also be emphasized that not every resident has the opportunity to use electronic tools, which leads to digital exclusion, affecting mainly older people. Additionally, the possibility of using specific features of new technologies and the properties of public media to manipulate public opinion should be considered (Porębski, 2020). For these reasons, electronic communication tools seem to be most effective when they complement existing budgeting procedures, that is, when they are one of the elements of a hybrid 'control and repair' system (Peixoto & Fox, 2016).

This article uses a chronological-problematizing structure because it reflects both the changes in the use of modern electronic tools over the years and shows what Schulz & Newig (2015) have defined as the need to rethink such technologically supported participation. The few scholarly studies conducted in Poland on the use of modern technologies in participatory budgeting have shown, among other things, that modern technologies and traditional ways of communicating in participatory budgeting are not separate (Zawadzka-Pąk, 2022). This study aims to analyse participatory/civic budgets in Poland in terms of the use of electronic communication tools. Several research questions were formulated during the research process: (1) At what stages of conducting a participatory/civic budget are electronic tools used (e.g. is it possible for residents to submit projects electronically; is it possible to vote electronically)? (2) What are residents' opinions on the electronic tools used in the participatory/civic budget in Warsaw? This study verifies the research hypothesis that the electronic tools used in the participatory/civic budgeting in Warsaw are gradually improving, and that the budget in this city is increasingly becoming an electronic one.

The research process mostly used primary sources (statistical data, legal acts, reports, and evaluation documents) and to a limited extent used scholarly studies. Deep-source analyses and comparative methods have also been used. The research was conducted on versions of the participatory/civic budget covering the Capital City of Warsaw. This was done for several reasons: first, Warsaw is the capital of Poland and largest city in Poland in terms of population; second, it is home to the main government offices and ministries, which makes it, at least theoretically, the place where new solutions are implemented on a large scale, including solutions in the field of e-democracy and e-participation; third, for political reasons, administrative decisions made in Warsaw are the subject of lively political and public discourse; fourth, the progress of individual versions of the participatory/civic budget is the subject of in-depth evaluation, carried out using surveys and interviews, among other things. All the participatory/civic budgets carried out in Warsaw were analysed during the research process.

This article consists of five sections. The first presents introductory issues; the second describes legal solutions connected with participatory budgeting in Poland. The third section evaluates the use of electronic tools in the first five versions of Warsaw's participatory budget. Subsequently, the fourth section analyses the use of electronic tools in the remaining six budgets, which was renamed the civic budget. Finally, the conclusion points out the positive and negative aspects of using electronic communication tools in the practice of participatory/civic budgeting in Warsaw.

1. Legal solutions

Until 2018, there were no statutory regulations on the functioning of participatory/civic budgets in Poland. Legal solutions contained in various acts were used. Usually, participatory/civic budgets were created based on Article 5a of the Act of 8 March 1990 on Municipal Self-Government (Sejm RP, 1990). Pursuant to Article 5a, paragraph 2, the local council has the power to establish the procedures and rules for conducting consultations on matters important to the community, and participatory/civic budgeting was treated as important. Therefore municipalities could adopt local laws regarding the principles of creating a participatory/civic budget. In other words, each community could adopt its own rules regarding submitting projects to the participatory/civic budget, as well as the methods of consulting on and selecting them. Financial resources allocated within such a budget could be assigned to implementing projects covering the statutory tasks of a given territorial unit. Therefore the procedures were optional and depended entirely on the decisions of the authorities of a given local government section. Individual units defined the conditions and scope of the participatory/civic budget and the pool of financial resources allocated for the implementation of the adopted projects.

In November 2017, a parliamentary draft act to amend certain acts in order to increase citizens' participation in the process of electing, functioning, and controlling certain public bodies was submitted to the Sejm (Poselski projekt ustawy o zmianie niektórych ustaw, 2017). Among other things, it concerned regulations on participatory/civic budgets. The Act was enacted on 11 January 2018, and the acts on municipal, district, and voivodeship self-government were amended. Thus the institution of civic/participatory budgeting as an obligatory form was anchored in legal provisions. According to the amendment, the civic/participatory budget was recognized as a special form of public consultation. The amended Act of 8 March 1990 on municipal self-government adopted a solution according to which, as part of the civic budget, residents decide annually in direct voting on part of the expenses of the municipal budget (Sejm RP, 1990). Tasks selected as part of the civic budget are included in the municipal budget resolutions. In the course of working on the draft budget resolution, a local council may not remove or significantly change the tasks selected under the civic budget. Municipalities with county rights are obliged to create a participatory budget. The amount of such a budget cannot be lower than 0.5% of the community's expenditure, as calculated based on the last submitted budget implementation report. There are 66 such cities in Poland. The financial resources spent under the participatory/civic budget can be divided into: 1) pools covering the entire community and its parts in the form of auxiliary units or groups of auxiliary units, and 2) project amount categories covering the entire community or part thereof (Article 5a, point 6). The local council is obliged to prepare a resolution containing detailed formal requirements that the submitted project must meet, the required number of sig-

natures under the project (which cannot be greater than 0.1% of the inhabitants of the area covered by the civic budget in which the project is submitted), and rules for assessing submitted projects (compliance with the law, technical feasibility, meeting formal requirements, appeal procedure, rules for carrying out voting, determining the results, and making them known to residents) (Article 5a, point 7).

In March 2022, the Sejm amended the Act on Municipal Self-Government (Sejm RP, 1990). Under Article 5a, point 6, funds spent under the civic budget may be divided into pools covering the entire community and its parts or categories of amounts for projects covering the entire area of the community or its parts. The new provisions were first applied during public consultations on budgets for 2023, when the submission of participatory/civic budget projects in a given community had not been completed.

2. Participatory budgeting in Warsaw

Participatory budgeting in Warsaw includes the following stages: development of a procedure, information and educational campaigns (including discussions about the district's needs), development and submission of projects, initial verification of projects, discussion of projects, selection of projects for verification (pre-selection), detailed verification, promotion of projects submitted to a residents' vote, selection of projects for implementation, and evaluation process.

In the first budget, the website www.twojbudzet.um.warszawa.pl was launched. One way to submit a project was to send it to the email address of the relevant district office. A list of positively verified projects, along with the changes introduced, was published online. If the project was withdrawn, the project promoter notified the appropriate organizational unit of the district office via email. A list of projects selected for resident voting was announced on these sites, and voting was possible electronically. In this case, it was necessary to have an active email account. However, the condition for a vote to be recognized was to open the link sent by Warsaw City Hall to confirm one's participation. The voting results and lists of projects to be implemented were published on the website. The recommendations indicated in the evaluation documents did not raise the issue of electronic tools being used to conduct participatory budgeting (Gójska et al., 2014).

The regulations regarding the second version of the participatory budget in 2016 referred to the ESOG (Elektroniczny System Obsługi Głosowania – Electronic Voting Service System) platform (Prezydent Miasta Stołecznego Warszawy, 2014). Thus an electronic system was developed to facilitate the participatory budgeting process. This system allowed users to use the following functionalities: submitting ideas; viewing submitted ideas, including attachments; commenting on the content published on the system, including the content of submitted projects; voting for projects;

and checking the implementation status of projects selected for voting. The website www.twojbudzet.um.warszawa.pl contained the basic information, and an official Facebook profile was integrated into the website. It can be emphasized that the profile functioned as a newsletter for people who had a Facebook account and were interested in current news. Moreover, the grassroots initiative of an open discussion group on participatory budgeting in Warsaw was created on social media and enjoyed great interest among residents.

Evaluation documents of this second version of the budget indicated that the website was the main knowledge channel for project authors; however, social media played a significant role (SACADA, 2015, pp. 27, 32). The electronic system was assessed positively, considering the understandability of the content, ease of use, aesthetics, and transparency (SACADA, 2015, p. 50). Among all the respondent groups, those aged up to 18 years old rated the ease of use of the voting system the best; the average ease of use decreased slightly with age. Respondents in the oldest age group rated ease of use the lowest among all groups, but this rating remained high on an overall scale. The transparency of the online voting system was rated the lowest among all age groups. Some respondents pointed out the difficulty in finding a specific project (SACADA, 2015, p. 50); in their opinion, it would be easier to build a search engine for projects using words and to search for an area by street addresses. This suggestion was also made by residents via emails sent to the office, which suggested introducing the possibility of searching for projects using 'tags'. The respondents also claimed that online voting required many clicks, an opinion shared by members of the districts' participatory budgeting teams (SACADA, 2015, p. 50).

The problem in the case of online voting was vote activation, that is, confirmation via email (SACADA, 2015, p. 51). Younger children who voted did not have email addresses. As for the activation links, they did not always reach the email addresses entered. During the evaluation, many of the email addresses provided by residents were found to be inactive or incorrect. Despite the highlighted 'confirm your vote' information on the website, not all residents noticed this message. Comments were also made regarding the impossibility of using one email address multiple times (SACADA, 2015, p. 51). It should be emphasized that the evaluation of the electronic tools used in the participatory budgeting was the most in-depth of all evaluations of the ten budgets.

In the 2017 budget, electronic communication was more visible on a larger scale. The posts appeared on www.facebook.com/groups/budzetwaw and on the official website www.twojbudzet.um.warszawa.pl; the email address used was twojbudzet@um.warszawa.pl. This information was also posted on district websites dedicated to participatory budgeting (Leszczyńska et al., 2016, p. 21). The electronic system developed for the purposes of conducting the participatory budgeting in Warsaw was rated better in this year than in the second year (Leszczyńska et al., 2016, p. 55). The idea of automatically deducting the costs of selected projects from the total sum and

marking which items were or were not still available was evaluated positively. The online voting system was assessed as being intuitive and simple (Leszczyńska et al., 2016, p. 55). There was also a positive reaction to the solution of sending an email in the event of an incomplete vote.

Based on the evaluation of the 2018 participatory budget, it can be concluded that the traditional method of voting was most often used by people over 50 (Huras et al., 2017, p. 16). Voters believed that the electronic voting system was aesthetic, transparent, easy to use, and had understandable content (Huras et al., 2017, pp. 16–17). The vast majority of the surveyed residents did not notice any technical problems while voting.

In the 2019 participatory budget, projects could be submitted, among others through the electronic participatory budget system available at www.app.twojbudzet.um.warszawa.pl (Centrum Komunikacji Społecznej Urzędu m.st. Warszawy, 2018, p. 25). This budget saw a reduction in the number of projects submitted (Makurat et al., 2018, p. 17). Voting was in electronic form, among others, using the electronic voting tool app.twojbudzet.um.warszawa.pl (Centrum Komunikacji Społecznej Urzędu m.st. Warszawy, 2018, p. 47). In this case, it was necessary to have (or set up) an email. A maximum of three people could vote using the same email address. The results of the participatory budgets in Warsaw are shown in Table 1.

Table 1. Participatory budgeting versions in Warsaw.

Versions	Electronically submitted projects in %	Number of voters	Electronic voting in %
1 (2015)	-	166,893	72.33
2 (2016)	68	172,395	58.91
3 (2017)	77	128,406	95.00
4 (2018)	84	117,381	95.00
5 (2019)	84	89,807	95.00

Source: Own work based on https://um.warszawa.pl/waw/bo/poprzednie-edycje

In 2015, electronic voting accounted for 72.33% of all votes. In 2016, there was a decrease to 58.91%. Since 2017, the share of electronic voters has increased rapidly, and stabilized at a very high level of 95% in 2017, 2018, and 2019. Since 2017, almost all voters have used the electronic form, suggesting a lasting change in residents' preferences and the effective digitalization of the participatory budget process. This seems to be the result of the widespread digitalization of everyday life and the increasing availability of the internet and mobile devices in particular. It should be noted that despite the growing percentage of electronic votes, the total number of voters has been decreasing year by year (from 172,395 in 2016 to 89,807 in 2019),

which may indicate other challenges to participation unrelated to the availability of the electronic voting system.

During the pandemic, many public, educational, and social services moved online. Often out of necessity, people began to use digital tools, breaking down previous barriers and resistance to new technologies. The pandemic meant that even people who were less digitally savvy had to learn how to use the internet for work, study, shopping, or contacting government offices; this translated into a greater openness to online voting. The analysed data on the first five years of the participatory budget in Warsaw show that even before the pandemic, the share of electronic voting in Warsaw was very high (95% from 2017 to 2019). The pandemic may have further consolidated this trend, making online voting the obvious choice for most residents.

3. Civic budgeting in Warsaw

The sixth version of the budget, in 2020, was based on the new legal provisions. Moreover, the name of the budget was changed to 'civic'; supporters of changing the name claimed that the new name was more understandable for residents. Previously, when submitting applications, it was not necessary to provide an identification number (PESEL), so foreigners could submit projects. According to the new rules, each resident could vote only once; therefore a PESEL number had to be provided for identification purposes, and foreigners could not vote for projects under civic budgets (Centrum Komunikacji Społecznej Urzędu m.st. Warszawy, 2019, p. 7). Such solutions still exist in practice today. Projects could be submitted in traditional or electronic forms, and residents could vote online on app.twojbudzet.um.warszawa.pl. Twenty additional electronic voting points were organized throughout the city, including in local activity centers, libraries, and community centres (Centrum Komunikacji Społecznej Urzędu m.st. Warszawy, 2019, p. 16).

A city discussion forum was created on app.twojbudzet.um.warszawa.pl. However, opinions regarding the functioning of the forum were negative: respondents complained about the lack of real discussion and low interest in the subject matter. A lack of moderation or a discussion supervisor were also mentioned as weaknesses. In the opinion of the project authors, the office should have been more involved in this discussion. Some people pointed out that the website was not working properly and that comments were insufficiently visible, which was not conducive to starting a discussion (Ośrodek Ewaluacji, 2019, pp. 47–48). As for the Facebook pages, the critical opinions were similar to those regarding the city website: no substantive discussion or no discussion at all, so-called hate, and little involvement in significant conversation. It was also pointed out that, compared to the website, the Facebook page was not a place for serious discussions (Ośrodek Ewaluacji, 2019, p. 49).

The evaluation interviews also revealed problems with online voting (Ośrodek Ewaluacji, 2019, p. 58). People expressed surprise that it took so long to thoroughly familiarize themselves with at least one project. The individuals were disappointed with the technical aspects of the online voting system; among other things, they pointed out an unintuitive interface and inconvenient filtering. Recurring technical difficulties were reported, such as a broken voting link, an error causing the list of district projects to be empty, problems with entering a postal code, and inaccuracies in the designation of project types (such as 'health' and 'healthcare') (Ośrodek Ewaluacji, 2019, p. 61).

During the seventh budget, for 2021, 17 additional electronic voting points were organized throughout the city. Due to the Covid pandemic, the ceremonial gala did not take place, and the results were published on the website. The promotional campaign used, among others, announcements on the civic budget website app.civicbudget.um.warszawa.pl, mailing, and posts on social media (Facebook) and on internet portals (Centrum Komunikacji Społecznej Urzędu m.st. Warszawy, 2020, p. 24). Regarding technical issues, it was pointed out that the power of servers should increase on the day at the end of voting. It was emphasized that electronic voting is difficult and excludes people who are less digitally competent, and searching for projects is not intuitive (Urbanik & Wilk, 2021, p. 9).

The opening meeting for the eighth version of the civic budget in Warsaw was organized online on the Zoom platform, due to the epidemiological restrictions. Online meetings dedicated to the new project authors were also organized. A new functionality was made available on the website https://bo.um.warszawa.pl/, the ability to generate posters and graphics encouraging voting for a given project. Each resident, without logging into their account, could download promotional material in various formats, including an A4 poster or a graphic for Facebook (Centrum Komunikacji Społecznej Urzędu Warszawy, 2021, p. 21).

The opening meeting for the ninth version of the budget was also organized online on Zoom (Centrum Komunikacji Społecznej Urzędu m.st. Warszawy, 2022, p. 8). As in the previous year, online meetings dedicated to new project authors were organized, and as before, the civic budget week was organized entirely online (Centrum Komunikacji Społecznej Urzędu m.st. Warszawy, 2022, p. 10). The promotional campaign was conducted on the bo.um.warszawa.pl website (Centrum Komunikacji Społecznej Urzędu m.st. Warszawy, 2022, p. 22); all interested persons could generate posters and graphics to encourage people to vote for a given project. Residents could again download promotional material in various formats without logging into their accounts, including an A4 poster or a graphic for Facebook. To make it easier for project developers to distribute posters in urban spaces, an interactive map of places (poles, noticeboards, and shop windows) was prepared (on google. com/maps) where authors could hang their promotional materials.

During the evaluation phase of the tenth anniversary version of the civic budget in 2024, residents submitted comments. Among other things, confusion about project numbers at different stages of the budget was reported to be a problem, and the existence of two websites about the civic budget in Warsaw was considered confusing (Centrum Komunikacji Społecznej Urzędu m.st. Warszawy, 2023, p. 2). The problem with hate speech in discussions about projects on the website was highlighted (Centrum Komunikacji Społecznej Urzędu m.st. Warszawy, 2023, p. 3). The introduction of forum regulations, more stringent moderation, or the de-anonymization of comment authors was proposed to address this issue; one idea was to introduce the requirement of first and last names for logging in. Regarding voting, the lack of the possibility of voting with a trusted profile (a free tool that allows to confirm the identity online without the need to visit an office in person) was reported as a problem, which is important for people who, for example, do not want to provide their PESEL number for security reasons (Centrum Komunikacji Społecznej Urzędu m.st. Warszawy, 2023, p. 4).

During the evaluation phase of the 2025 civic budget of the 11th version of the civic budget, residents submitted comments on the budget. In relation to the project submission stage, an idea emerged for a tool in the form of a map that would suggest to project developers the location in which a project could be implemented (Centrum Komunikacji Społecznej Urzędu m.st. Warszawy, 2024a, p. 1). The tool 'How much does the city cost?' was assessed positively; however, a need for its systematic updating was emphasized (Centrum Komunikacji Społecznej Urzędu m.st. Warszawy, 2024a, p. 1). Electronic or paper voting was considered insufficient; an idea was proposed to create voting points in the urban space. In relation to the voting stage, the introduction of the possibility of searching for projects on the website, using the ESOG number for which the user wants to vote, was postulated. Digital exclusion was also observed; the development of a solution that would counteract digital exclusion and enable all residents of Warsaw to vote was suggested (Centrum Komunikacji Społecznej Urzędu m.st. Warszawy, 2024a, p. 5). A problem was also reported regarding the lack of access to the bo.um.warszawa.pl website when outside Poland (Centrum Komunikacji Społecznej Urzędu m.st. Warszawy, 2024b, p. 2). The results of the versions of civic budgeting in Warsaw are shown in Table 2.

Table 2. Civic budgeting versions in Warsaw.

Versions	Electronically submitted projects in %	Number of voters	Electronic voting in %
6 (2020)	88	105,822	99.0
7 (2021)	88	109,025	99.6
8 (2022)	92	93,539	99.4
9 (2023)	92	88,861	99.0

10 (2024)	93	85,048	99.2
11 (2025)	93	75,657	99.4

Source: Own work based on https://um.warszawa.pl/waw/bo/poprzednie-edycje

The six civic budgets in Warsaw from 2020 to 2025 took place under different formal and legal conditions, with changed the nomenclature: the participatory budget was renamed as 'civic'. The share of online submissions increased from 88% in 2020 to 93% in 2024 and 2025. There was also a clear drop in the number of voters, from 105,822 in 2020 to 75,657 in 2025. This indicates a drop of over 28% during the six years, which may indicate fatigue with the participatory budget formula or other barriers to participation in the programme. The percentage of people voting electronically increased from 99% in 2020 to 99.6% in 2021 and then remained at a very high level (99–99.4%) in subsequent years. In practice, almost all voting occurs online, confirming a permanent change in social habits. Both project submissions and voting are almost entirely electronic processes; this is the result of technological and social changes, reinforced by the Covid-19 pandemic.

Conclusions

This study aimed to analyse the participatory/civic budget in Warsaw in terms of the use of electronic communication tools. Therefore two research questions were formulated: (1) At what stages of conducting a participatory/civic budget are electronic tools used? (2) What are the residents' opinions regarding electronic tools used in participatory/civic budgeting in Warsaw? The research process verified the research hypothesis that the electronic tools used in the participatory/civic budget in Warsaw are being gradually improved, and that the budget in the city is increasingly becoming an electronic one. The analysis of 11 years of the participatory/civic budget in Warsaw allows both the research questions and the research hypothesis to be addressed.

Referring to the first research question, it should be stated that electronic tools have been used to conduct participatory/civic budgeting in Warsaw. They are primarily used in the project submission and voting phases, and interest in the use of electronic tools in both phases is increasing every year. Recently, they have also been used in the promotion phase for submitted projects, while attempts have been made to use electronic communication tools to enhance deliberation in the budgeting process. However, as demonstrated, users criticized the level of debate both on dedicated platforms and on Facebook. The research has shown that the biggest problem related to participatory/civic budgeting is the low interest of residents. The voting turnout is also low, amounting to approximately a dozen or so per cent of the total population. Electronic tools can support the process of educating residents and raising their level of awareness related to the participatory/civic budget. Changes in the regulations for

conducting the budget, as well as changing the name, generally do not support interest in participating in the preparation of a project or projects or in voting. We should therefore expect greater transparency in terms of formal and legal solutions. The Covid-19 pandemic has increased interest in the use of electronic tools in budgeting.

To answer the second research question, it should be stated that residents' opinions about the electronic tools were divided. Criticisms were generally directed at websites, and the voting system was perceived as being unintuitive. The discussion site was criticized for lacking proper moderation. However, it should be noted that the tools have gradually improved. On the one hand, the overwhelming majority of residents in Warsaw use electronic communication tools in the budgeting process, which undoubtedly makes it easier for them. On the other hand, however, the use of electronic communication tools is generally not a significant factor in increasing resident participation in local decision-making.

During the research process, the research hypothesis – the electronic tools used in the participatory/civic budget in Warsaw are gradually improving, and the budget in this city is increasingly becoming an electronic one – was partly verified positively. On the one hand, electronic tools are commonly used in every phase of the participatory/civic budget. However, there are problems with these electronic tools for many residents, and there are some residents who are not familiar with them; this is why some respondents stated the digital exclusion of some residents. The research also shows that the participatory/civic budget in Warsaw is in fact a tool of participatory democracy for residents who want to take part; however, it can only be considered a tool for deliberative democracy to a limited extent. The use of electronic communication tools has not changed this.

REFERENCES

Allegretti, G. (2014). Paying attention to the participants' perceptions in order to trigger a virtuous circle. In N. Dias (Ed.), *Hope for democracy: 25 years of participatory budgeting worldwide* (pp. 47–63). https://partycypacjaobywatelska.pl/wp-content/uploads/2018/10/hope_for_democracy_-_25_years.pdf

Bateman, G. R. (2020). *The transformative potential of participatory budgeting: Creating an ideal democracy*. Routledge.

Centrum Komunikacji Społecznej Urzędu m.st. Warszawy. (2015). *Raport z konsultacji społecznych z mieszkańcami m.st. Warszawy w zakresie budżetu partycypacyjnego na rok 2016*. https://um.warszawa.pl/waw/bo/2-edycja

Centrum Komunikacji Społecznej Urzędu m.st. Warszawy. (2018). *Raport z konsultacji społecznych z mieszkańcami m.st. Warszawy w zakresie budżetu partycypacyjnego na rok 2019*. https://um.warszawa.pl/waw/bo/5-edycja

Centrum Komunikacji Społecznej Urzędu m.st. Warszawy. (2019). *Raport z konsultacji społecznych z mieszkańcami m.st. Warszawy w zakresie budżetu obywatelskiego na rok 2020*. https://um.warszawa.pl/waw/bo/6-edycja

Centrum Komunikacji Społecznej Urzędu m.st. Warszawy. (2020). *Raport z konsultacji społecznych z mieszkańcami m.st. Warszawy w zakresie budżetu obywatelskiego na rok 2021*. https://um.warszawa.pl/waw/bo/7-edycja

Centrum Komunikacji Społecznej Urzędu m.st. Warszawy. (2021). *Raport z konsultacji społecznych z mieszkańcami m.st. Warszawy w zakresie budżetu obywatelskiego na rok 2022*. https://um.warszawa.pl/waw/bo/8-edycja

Centrum Komunikacji Społecznej Urzędu m.st. Warszawy. (2022). *Raport z konsultacji społecznych z mieszkańcami m.st. Warszawy w zakresie budżetu obywatelskiego na rok 2023*. https://um.warszawa.pl/waw/bo/9-edycja

Centrum Komunikacji Społecznej Urzędu m.st. Warszawy. (2023). *Podsumowanie 10. edycji budżetu obywatelskiego. Notatka ze spotkania online, które odbyło się 17 lipca 2023 r*. https://um.warszawa.pl/waw/bo/-/podsumowanie-10-edycja

Centrum Komunikacji Społecznej Urzędu m.st. Warszawy. (2024a). *Podsumowanie 11. edycji budżetu obywatelskiego 23 lipca 2024. Notatka ze spotkania*. https://um.warszawa.pl/waw/bo/11-edycja-na-rok-2025

Centrum Komunikacji Społecznej Urzędu m.st. Warszawy. (2024b). *Podsumowanie 11. edycji budżetu obywatelskiego 25 lipca 2024. Notatka ze spotkania online*. https://um.warszawa.pl/waw/bo/11-edycja-na-rok-2025

Friess, D., Escher, T., Gerl, K., & Baurmann, M. (2021). Political online participation and its effects: Theory, measurement, and results. *Policy & Internet*, *13*(3), 345–348.

Gójska, A., Lewenstein, B., Pogoda, I., & Zielińska, E. (2014). *Rekomendacje do organizacji budżetu partycypacyjnego w Warszawie na 2016 rok (proces realizowany w 2015 roku), lipiec 2014*. https://um.warszawa.pl/waw/bo/1-edycja

Huras, P., Przybył, C., Bieńkowska, Z., Chojecki, J., Grajek, A., Kamińska, A., Matysiak, M., Nowińska, K., & Pałka, S. (2017). *Badanie ewaluacyjne IV edycji budżetu partycypacyjnego w kontekście mieszkańców zaangażowanych w proces. Warszawa, wrzesień 2017*. https://um.warszawa.pl/waw/bo/4-edycja

Kębłowski, W. (2013). *Budżet partycypacyjny. Krótka instrukcja obsługi*. Instytut Obywatelski.

Lerner, J. (2014). *Everyone counts: Could 'participatory budgeting' change democracy?* Cornell University Press.

Leszczyńska, M., Pogoda, I., & Szostakowska, M. (2016). *Ewaluacja procesu budżetu partycypacyjnego w Warszawie na rok 2017. Raport końcowy. Warszawa, wrzesień 2016*. https://um.warszawa.pl/waw/bo/3-edycja

Makurat, M., Charchuła, Z., & Wałaszek, J. (2018). *Badanie ewaluacyjne V edycji budżetu partycypacyjnego w Warszawie. Raport końcowy. Warszawa 2018*. https://um.warszawa.pl/waw/bo/5-edycja

Marczewska-Rytko, M. (2024a). Demokracja bezpośrednia i deliberatywna: Analiza porównawcza idei, instytucji, rozwiązań formalnoprawnych oraz praktyk. In J. Podgórska-Rykała & P. Pospieszna (Eds.), *Innowacje deliberatywne. Inspiracje dla praktyków i teoretyków* (pp. 9–30). C. H. Beck.

Marczewska-Rytko, M. (2024b). Budżet obywatelski/partycypacyjny jako forma uczestnictwa obywateli w procesie decyzyjnym w Polsce. *Horyzonty Polityki*, *15*(51), 269–286.

Marczewska-Rytko, M., & Maj, D. (2021). *Civic/participatory budget in V4 countries in the context of good practices*. Maria Curie-Skłodowska University Press.

Ośrodek Ewaluacji. (2019). *Badanie ewaluacyjne VI edycji budżetu obywatelskiego w Warszawie. Raport końcowy*. https://um.warszawa.pl/waw/bo/6-edycja

Peixoto, T., & Fox, J. (2016). When does ICT-enabled citizen voice lead to government responsiveness? *IDS Bulletin*, *47*(1), 23–40.

Porębski, L. (2020). O dialogu bota z trollem. Partycypacja polityczna w okresie rewolucji informacyjnej. In M. Marczewska-Rytko & D. Maj (Eds.), *Partycypacja polityczna* (pp. 19–28). Wydawnictwo Uniwersytetu Marii Curie-Skłodowskiej.

Poselski projekt ustawy o zmianie niektórych ustaw w celu zwiększenia udziału obywateli w procesie wybierania, funkcjonowania i kontrolowania niektórych organów publicznych. (2017). https://www.sejm.gov.pl/Sejm8.nsf/PrzebiegProc.xsp?nr=2001

Prezydent Miasta Stołecznego Warszawy. (2014). *Regulamin przeprowadzania budżetu partycypacyjnego w Mieście Stołecznym Warszawie na rok 2016. Załącznik do zarządzenia nr 6699/2014 Prezydenta Miasta Stołecznego Warszawy z dnia 16 października 2014 r*. https://um.warszawa.pl/waw/bo/2-edycja

SACADA Pracownia Badawczo-Projektowa. (2015). *Ewaluacja budżetu partycypacyjnego w m.st. Warszawie na rok 2016 raport końcowy. Kraków, wrzesień 2015*. https://um.warszawa.pl/waw/bo/2-edycja

Schulz, D., & Newig, J. (2015). Assessing online consultation in participatory governance: Conceptual framework and a case study of a national sustainability-related consultation platform in Germany. *Environmental Policy and Governance*, *25*(1), 55–69.

Sejm RP (1990). Ustawa z dnia 8 marca 1990 roku o samorządzie gminnym (t.j. z 2023 r. poz. 40, 572, ze zm.).

Sintomer, Y., Röcke, A., & Herzberg, C. (2016). *Participatory budgeting in Europe: Democracy and public governance*. Routledge.

Sroka, J., Pawlica, B., & Ufel, W. (2022). *Ewolucja budżetu obywatelskiego w Polsce – w kierunku deliberacji czy plebiscytu?* Wydawnictwo Libron.

Troitiño, D. R. (2022). The European Union facing the 21st century: The digital revolution. *TalTech Journal of European Studies*, *12*(1), 60–78.

Urbanik, A., & Wilk, W. (2021). *Podsumowanie budżetu obywatelskiego na 2021 rok. Notatka ze spotkań*. https://um.warszawa.pl/waw/bo/7-edycja

Wampler, B., McNulty S., & Touchton, M. (2021). *Participatory budgeting in global perspective*. Oxford University Press.

Zawadzka-Pąk, U. K. (2022). Participatory budgeting as the instrument of technologically supported dialogue in Cracow, Poland. *TalTech Journal of European Studies*, *12*(2), 3–19.

Zawadzka-Pąk U. K., & Tomáškova, E. (2019). Legal and axiological aspects of participatory budgeting procedure in Poland and the Czech Republic. *Białostockie Studia Prawnicze*, *24*(3), 165–175.

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

sciendo

DOI: 10.15290/bsp.2026.31.01.16

Received: 13.08.2025
Accepted: 13.12.2025

Anna Pacześniak
University of Wroclaw, Poland
anna.paczesniak@uwr.edu.pl
ORCID ID: 0000–0002–4782–4432

Digitalization of Political Parties in Poland: Between Law and Practice

Abstract: Analysis of political parties' digital adaptation is a rapidly growing field of research that was accelerated by the COVID-19 pandemic. This study of seven political parties in Poland, using the operationalization proposed by the DIGIPART project, provides information on the specifics of the external and internal use of digital tools in a young democracy. The main sources of data for the dataset are party websites, apps, social media and online participation platforms, which have been subjected to qualitative content analysis. The analysis confirms that the digitalization of parties is more advanced in external dimensions that directly connect parties with voters (the communication and resources pillar) than in dimensions related to internal party procedures (the electoral, deliberative and participatory pillar). The use of digital tools is influenced more by the level of intra-party democracy and the party's distance from the centre on the right–left axis than by age or party size.

Keywords: digitalization, party organization, party communication, Poland

Introduction

Change is written into the DNA of political parties. In order to survive in the political market, a party must identify and understand changes in its environment, respond to them accordingly and be adaptable. The technological and communicative progress of the turn of the millennium brought with it a significant increase in the popularity and use of digital tools in all spheres of social life (Giovanola, 2023; González-Cacheda & Cancela, 2024, p. 489; Rek, 2024; Troitiño, 2022) and is seen as one of the main reasons for undertaking new forms of collective and individual action in politics. Bennett and Segerberg (2013) describe this change as a transition

from a logic of collective action to a logic of connective action. As information and communication technologies influence the way people engage in politics, political parties are trying to adapt to the new reality (Jacuński, 2022, p. 108). While some of them underwent digital transformation fairly quickly, others experienced organizational inertia that slowed down the adaptation process (Ziegler et al., 2024). Although most parties have embraced new technologies to connect with and reach out to citizens, only a small proportion of them have used digital tools to make internal decisions virtually. One of the reasons for the far-reaching reluctance of political parties to implement new technologies for internal organizational management may be the fact noticed by Poguntke et al. that 'meetings without physical presence fundamentally change the nature and logic of decision-making' (2021, p. 15).

The challenges associated with party digitalization turned into opportunities during the COVID-19 pandemic; the need for social distancing and pandemic restrictions forced parties to transform in order to fulfil their functions. During this particular period, all political institutions had to implement remote communication tools; otherwise they would have had to suspend their daily activities. While some parties limited the number of delegates at party congresses or shifted decision-making from party congresses to smaller, less inclusive bodies, others decided to postpone previously planned events until pandemic restrictions were eased, recognizing that a remote congress or policy convention would not fulfil all their functions; still others turned to digital mechanisms with greater confidence (Poguntke et al., 2021, pp. 15–16). The Polish research team of the Political Party Database Project collected data on this question during the pandemic, so it is worth returning to the same political parties after a few years to check the extent to which the tools and practices implemented at that time are still used in the functioning of the organization, and what has been abandoned after the lifting of state restrictions.

The aim of this article is to investigate the level of digital adaptation of Polish political parties, as most of the research to date has focused on parties operating in countries with a longer democratic tradition than those in Central Europe. Two research questions are formulated: (1) how and for what purpose parties in Poland use digital tools, and (2) which party organizations are more inclined towards digital adaptation and which are more cautious in this regard. The corpus of political entities analysed here includes seven parties with representation in the lower house (Sejm), which are ideal for comparison due to their diversity in terms of age, size, parliamentary strength and position on the political scene.

The paper is organized as follows: in the first part, I analyse the existing literature on the internal and external dimensions of the digitalization of political parties and present the analytical framework adopted in the article. Next, I provide basic information about the parties that constitute the case study; subsequently, I present descriptive results of the dataset. In the last section, I discuss the implications of the findings and the contribution to the existing literature.

1. Internal and external use of digital tools in party organizations

The adaptation of political parties to the new digital environment has given impetus to researchers on the parties, especially in the context of the previously diagnosed process of party organizations becoming distanced from society. The changing role of political parties in democratic regimes is driven by the perceived disconnection and an increasing gap between the representatives and the represented (Mair, 2013). Their traditional role as a so-called transmission belt between society and the state has been significantly diluted. Most parties are losing their membership bases, with the result that their social embeddedness is being eroded (Scarrow & Gezgor, 2010). In this context, digital technologies and the internet are perceived as a means to create new methods of connecting political parties with their social bases (Gibson et al., 2018). Examples of this include new membership options, such as 'sympathizers' or 'party friends', allowing registered supporters to participate in intra-party ballots or recruiting supporters as virtual members of online forums (Ponce & Scarrow, 2016, p. 679). The growth in the number and functions of digital platforms, which has enabled parties 'to interact, mobilize resources and open up new participatory processes aimed at their grassroots' (González-Cacheda & Cancela, 2024, p. 489), has led some authors to focus on the potential of digital tools to increase participation and interaction between political parties and citizens. Peña (2021) coined the term 'activist party' to describe party organizations that, taking advantage of the increasing opportunities of digital technologies, make policies and organizational choices that combine the arenas of social movements and political parties to strategically gain traction with members and voters.

The second strand of research on party digitalization concerns the use of digital platforms for internal organization management and their impact on intra-party democracy and power distribution. In recent years, there has been a trend within some parties towards increasing internal democracy (Cross & Katz, 2013) by giving individual members new rights and powers, such as selecting party candidates (Barnea & Rahat, 2007) or party leaders (Cross & Gauja, 2019) or influencing party policies (Scarrow & Gezgor, 2010, p. 826). Digital platforms enable quick ad hoc consultations with members on current political issues and facilitate internal party referendums, which results in a shift towards the plebiscitary variant of intra-party democracy and away from an assembly-based model, which promotes deliberation to a greater extent than simply voting on previously proposed solutions (Poguntke et al., 2016, pp. 670–671).

The existing literature shows that parties are more inclined to digitize external processes, such as relations and communication with supporters (Dommett & Temple, 2018; Gibson & Ward, 2009), than to invest in digital improvements to the management of party organization (Invernizzi-Accetti & Wolkenstein, 2017, p. 104). This seems to be due to cost–benefit calculations. Failure to digitize externally would risk

losing electoral votes, while a lack of digital facilities within the organization has a much smaller impact on either the functioning of the party or its image.

Observation of changes occurring in parties resulting from the use of digital technologies has prompted some scholars to propose new party models, naming them cyber (Margetts, 2006) or digital parties (Deseriis, 2020; Gerbaudo, 2019; Jääsaari & Šárovec, 2021); this is exemplified by the Pirate parties, the Spanish Podemos, or the Italian Movimento 5 Stelle. However, it is increasingly pointed out that digitalization is a ubiquitous phenomenon involving most, if not all, party types and forms (Peña & Gold, 2023 p. 3258). The COVID-19 pandemic triggered more changes and forced virtually all parties 'to switch to online organizing, accelerating the adoption of platform-based technologies and web-based collaboration tools' (Ziegler et al., 2024, p. 252).

Early research on party digitalization has focused on individual case studies (e.g. Datts & Gerl, 2024; Gerbaudo, 2021), followed by small-scale comparisons, e.g. of political parties operating within the same party system or parties belonging to the same political family (e.g. Barberà et al., 2019; Correa et al., 2024; Oross & Tap, 2023; Pedersen & Saglie, 2005). More recently, analyses of trends in digitalization in a larger number of countries have been published (e.g. González-Cacheda & Cancela Outeda, 2024; Sandri et al., 2025). The prevalence of digital innovations implemented by parties has led to these issues being included in cross-national initiatives creating a comparative database of political party organizations, such as the Political Party Database Project (Scarrow et al., 2017). Alongside many other aspects to do with the performance of party organization, the latest round of this project collects data on the functionality of party websites in terms of external communication, mobilization of supporters, fundraising and the use of digital tools for party management.

Smaller in scope but entirely focused on the phenomenon that interests us in this paper, the Digitalisation in Parties Dataset (DIGIPART) presents the scope of digital platforms' application and their affordances within political parties in five Western European countries (Sandri et al., 2025). The DIGIPART research team provides the first extensive operationalization and comparative data collection of both the internal and external dimensions of using digital tools in the process of intra-party elections, recruitment and engagement of party members, fundraising, electoral campaigns and communication with supporters and voters. The DIGIPART research team has assumed that the digital transformation of political parties is not a linear and all-encompassing phenomenon, and propose five key dimensions (pillars) of this process: electoral, deliberative, participatory, resources and communication (Table 1).

Table 1. Dimensions and main variables of party digitalization.

Electoral pillar	Deliberative pillar	Participatory pillar	Resources pillar	Communication pillar
online voting (party leadership)	deliberative online platforms	online consultations	online fee payment	party website
online voting (candidates)	other deliberative online initiatives	online membership	online crowdfunding/ donations	social media, social networking sites, mobile instant-messaging services
online voting (party bodies)	party congresses digitalization	digital activities for electoral campaigns	official online store	other forms of online communication

Source: Sandri et al., 2025, p. 1761

Since no data on Polish parties was collected as part of the aforementioned project, regardless of the distinctive features of Polish political parties and the historical context of a young but already consolidated democracy, in this paper I will deliberately use exactly the same research framework. Its application will allow me to fill in a missing piece from a newer democracy in the map of the digitalization of party organizations in Europe.

2. Case selection and methods

The conclusions drawn from the literature on the digitalization of political parties suggest that this process does not occur with the same intensity in all parties and does not concern the same dimensions. It can be assumed that the age of the party and its size, political position and parliamentary representation may be significant. With this in mind, I have characterized the corpus of my analysed cases.

Even though the Polish party system is relatively young, as its formation was initiated by the democratic transition in Central and Eastern European countries in the late 1980s and early 1990s, its political parties are diverse in terms of age. The parties with the longest history are successor parties, formed on the basis of parties that functioned in the non-democratic system. Two such parties have survived to this day: the New Left (NL; formerly the Democratic Left Alliance) and the Polish People's Party (*Polskie Stronnictwo Ludowe*, PSL). The second group includes parties formed at the beginning of the 21st century which still dominate the Polish political landscape today, namely the Civic Platform (*Platforma Obywatelska*, PO) and the Law and Justice Party (*Prawo i Sprawiedliwość*, PiS). The youngest parties appeared on the Polish political scene in the second decade of the 21st century. In this analysis, I will only include those of the youngest parties that have survived at least two elec-

tions, i.e. the Together Party (*Partia Razem*, R), the Confederation (*Konfederacja*, K) and the Poland 2050 (*Polska 2050*, PL2050).

The political parties in the dataset also vary in size, as determined by the number of formal members. Generally in Poland, party membership remains low. Only the post-communist parties (i.e. the two oldest ones) inherited a relatively extensive membership base, while the others had to build theirs with great effort. Only the Polish People's Party managed to retain part of its membership and remains the largest party to this day. The second largest party is the Law and Justice, which, despite its initial restraint in expanding its base of grassroots activists (Pacześniak & Wincławska, 2017), became attractive, especially during its eight years in power between 2015 and 2023, and recently accepted many new members. The newest parties are the least numerous, although there are visible differences between them resulting from the adoption of different concepts for building an effective party organization. The Confederation, for example, has focused on building a base of supporters, reserving membership status almost exclusively for politicians representing the party in parliament and other political bodies. In contrast, the Together Party had several thousand members in its first few years of existence, but after the 2025 presidential election, when the party's candidate ran for the first time, it attracted around 10,000 new members, as reflected in Table 2.

Table 2. The characteristics of the analysed political parties.

Party	Year of creation	Membership	Percentage of parliamentary seats (first session of Sejm in 2023)	Political position
PSL	1990	73,222	6.9	Centre-right
NL	2021 (1999)	25,703	3.9	Centre-left
PO	2001	25,500	34.1	Centre-right
PiS	2001	48,000	41.3	Right
R	2015	12,000	1.7	Left
K	2019	90	3.9	Far right
PL2050	2021	848	6.9	Centre

Source: Author' elaboration based on Sejm, n.d. (parliamentary representation); Jędral, 2025 (party membership)

The parties analysed also vary in terms of their parliamentary representation, position on the right–left axis and current government status. As the latter changes due to the principle of alternation of power, it has not been included in Table 2.

The main data sources of the dataset were party websites, apps, social media and online participation platforms. I also subscribed to all possible party newsletters in order to compare the parties' communication promises with reality. In order to learn about the usefulness of digital tools in internal party management, concrete ques-

tions were sent to political parties. When contact with party headquarters proved ineffective (i.e. party representatives did not respond to two emails), I obtained information through less formal channels, contacting selected party members directly. Even though this is not a standard method of data collection, I decided that it was better to obtain data in this way than to remain without any data at all. This method of data collection carries the risk of obtaining unverified information and affecting the reliability of the results. The parties that did not respond to emails sent to their headquarters were the Confederation, the Poland 2050 and the Law and Justice.

3. Results: The further away from the centre, the better the digital adaptation

In this section I present the results of the analysis of each party, starting with those that use digital tools in the greatest number of dimensions and do so most consistently, and ending with those whose digital adaptation is weakest, random or unsystematic.

3.1. The Together Party

The most left-wing party in the Polish political landscape, remaining in opposition both to the United Right governments in 2015–2023 and to Donald Tusk's coalition government since 2023 (composed of the Civic Platform, the Poland 2050, the Polish People's Party, and the New Left), and with the smallest number of deputies in parliament, is the party that has implemented digital tools most extensively, both in internal relations and external communication. The electoral dimension of the digitalization of the party includes online voting for the party leadership and party bodies but not for candidates for national elections. The party strongly focuses on the active online participation of its members, offering them tools such as deliberative online platforms, online consultations and referendums. It promotes not only digital activities within the party (e.g. webinars, online training and information meetings with MPs), but also beyond it (such as digital initiatives promoting civic engagement, online petitions and protests). During electoral campaigns the party engages even more in digital activities (online canvassing, virtual meetings, message targeting). It is possible to send online donations but not membership fees; there is no official party store. The party congress is not digitalized nor streamed.

The party's communication pillar is the most developed. The Together Party has a website (in Polish, English and Ukrainian) and uses YouTube, social networking sites (Instagram, X, Facebook, Mastodon) and mobile instant-messaging services to contact members and sympathizers. There is no 'Contact' section on the website, but anyone can sign up to receive newsletters and emails from the party. Party information is sent out on average once a week, and much more frequently during election campaigns. The webpage gathers some application information about interested sup-

porters through an online form and promises 'someone will get back to you'; however, it is not possible to became a full member online.

3.2. The Confederation

Like the Together Party, the Confederation belongs to the youngest generation of Polish parties, but in terms of ideology, it occupies an extremely distant place, on the far right of the political scene. In popular perception, this group is the most effective in terms of its use of digital technologies. This belief stems from the fact that the party invests practically all its energy and resources in the most visible dimension of digitalization: external communication. The party has a website (as it is a nationalist group, it is only in Polish) and YouTube channel, and uses social networking sites (Instagram, X, Facebook, TikTok) and mobile instant-messaging services to contact sympathizers. Anyone can subscribe to the party's newsletter and receive selected news by logging on to the website. However, even during the 2025 presidential election campaign in which the party leader participated, the newsletter was not a communication tool frequently used with subscribers.

It is not possible to contact the party or download a membership form via the website; a mobile phone number and email address are provided for this purpose. This shows that the low size of the membership (less than 100 people) is not a coincidence: the party does not care about expanding its membership base, but instead relies on supporters. By contrast, there is no problem making an online donation to the party.

However, it is worth noting that the Confederation is a federal party, a coalition of several parties. They all have separate procedures, their own policies for communicating with supporters, and also structure their internal relations in their own way. For example, the New Hope party (*Nowa Nadzieja*), which is part of the Confederation, offers the possibility of becoming a party member online, although it does not have a dedicated gateway for paying membership fees.

3.3. The Poland 2050

One might expect that the Poland 2050, the youngest of the parties analysed, would consider the digital environment to be its natural habitat. This expectation also stems from the observations of the first presidential campaign of the party leader Szymon Hołownia, who made his political debut as a candidate in the 2020 election (Pacześniak, 2023, p. 1027–1028). After achieving a good result (over 13% of the vote and third place), he decided to capitalize on the mood and energy that had been awakened in society and founded his own party, the Poland 2050, in 2021. During the 2020 presidential campaign, the COVID-19 pandemic made it completely impossible for candidates to hold face-to-face meetings with voters; most communication and mobilization activities were therefore moved online. For a political newcomer who had no party structure behind him, whose funds were much more limited than those of his rivals, but who was adept at using social media, this proved to be a real boon.

Hołownia introduced a new style of communication in Polish politics. He broadcast live on Facebook every day to create the impression of building a personal relationship with each of his supporters. He also repeatedly stated that he wanted to hear the opinions of all Poles.

After he founded the party, the leader's declarations were turned into an experimental digital tool. In September 2021, the party announced the launch of a special app (called *Jaśmina* in Polish) that would allow registered supporters to co-create the party's programme by participating in direct online voting. It started with a single survey allowing users to express their opinions on the most important issues concerning Poland. There was also an aggregate of politicians' tweets, party programme documents and specialized analyses from many fields, as well as contact details for people and offices associated with the party leadership. It was also possible to search for other people and build a network of friends, which shows that it was intended to be a kind of new social network. After a few months, the application was shut down, and users saw an error message on their screens.

Currently, the Poland 2050 does not stand out in terms of digitalization among most Polish parties: it has a website and YouTube channel, and uses social networking sites (Instagram, X, Facebook). Content on social media is replicated, the YouTube channel is used irregularly, and activity only intensifies during election campaigns. The party's website features a 'Stay in touch' section, which allows users to subscribe to a newsletter promising to provide the latest information, keeping them up to date with the party's activities and the activities of parliamentarians and ministers. However, this promise has not been fulfilled, as after a few mails, I stopped receiving any information. Although there is also a 'Join us' section on the website, it is not possible to register with the party online; the website only allows an application form to be sent, after which the party will contact the user by phone. The most visible facility on the party website is the one that allows financial support for the party. It is the only red element on the site, marked with a beating heart icon. A dedicated payment gateway has been created, specific amounts are suggested and instructions are included on the conditions that must be met for the party to accept a donation.

In the Poland 2050, party leader elections are held online, as the public learned when the party founder's term was ending and his successor was being elected in January 2026. It turned out that digitising the internal procedure for electing the party leader could cause image problems for the party. During the second round of online voting, the IT systems failed. Some of the party's politicians speculated in the media that there had been an external attempt to disrupt the election process, and even that there might have been a cyberattack. The leadership elections were suspended, and the party plunged into a deep image crisis, which was also due to the fact that the public noticed a discrepancy between the policies proposed by the party (e.g. the introduction of universal online elections) and its inability to conduct internal party elections on a much smaller scale.

3.4. The Polish People's Party

The Polish People's Party is one of two successor parties analysed in my corpus, and the only one operating under the same name since the beginning of the democratic transition. Even though it is perceived by the public as a conservative party (which it is in ideological terms), and as traditional due to its rural electorate, the party presents an average level of adaptation to digital reality. The party has a website and YouTube channel, and uses social networking sites (Instagram, X, Facebook, TikTok). Content on social media is sometimes replicated, although it is clear that attempts are being made to diversify the message. YouTube is used irregularly and activity only intensifies during election campaigns, which seems to be almost the rule in Polish parties. Every member of the party's decision-making bodies has their own social media account, at a minimum on Facebook, but most also have Instagram and are active on X. All links are available on the party's website.

The party's website has a 'Contact' section that redirects to the email addresses and telephone numbers of local party offices. The party does not offer regular newsletters to supporters; this service is available to members only. It is not possible to register for the party online, but one can pay the membership fee or send a donation; a dedicated gateway for this has been created.

The Polish People's Party is committed to representative internal democracy and decision-making at congresses, which require personal attendance. Nevertheless, it regularly conducts consultations among its members using digital tools. In 2025, the party leadership polled activists twice in this way. In May, between the first and second rounds of the presidential election, the party leadership asked about support for the candidate put forward by the Civic Coalition, and in June about a possible change of coalition partner. Digital tools allow for a quick assessment of the mood within the party and give members the impression that they have an influence on the final decisions made by the leadership.

3.5. The Civic Platform

The Civic Platform uses digital tools mainly for external communication. It has a static website, fulfils the obligation to be present on YouTube and has accounts on social media platforms (Facebook, X, Flickr), although analysis of their content shows low engagement by moderators. Anyone can sign up on the party website to receive newsletters. The reality is less optimistic, as news is practically never sent outside of campaign periods. There is a 'Donate now' section on the party's website, but donations must be made via traditional bank transfer rather than a dedicated payment gateway. It is also not possible to join the party via the website, although it is possible to leave contact details and declare an interest in starting the membership procedure.

Even though the party does not use online tools to engage members in the day-to-day running of the party or internal discussions, it did use digital technology in the election process: in November 2024, the Civic Coalition held primaries to select a can-

didate for the presidential election. All members were eligible to participate in the vote via secure text message to choose one of two candidates selected by the leadership.

3.6. The New Left

The New Left is the second successor (post-communist) party analysed in the corpus, which changed its previous name, the Democratic Left Alliance, in 2021. The party has a website, where the first dynamic section is titled 'Join us'. This gives the impression of great openness to new members, but it is only possible to send a contact form or download a membership declaration to deliver in person. The rest of the content is very static, as if respecting the preferences of the older cohort of the electorate.

Two issues distinguish the New Left from the other parties analysed. It seems indifferent to raising funds, as its website does not have a section on support and there is no information on how to pay membership fees. Another characteristic feature is the party's YouTube channel, which is frequently updated with new content. Much of the credit for this goes to Magdalena Biejat, the left-wing candidate in the 2025 presidential election, who has maintained her campaign momentum and offers, for example, weekly political summaries, but other well-known politicians post their content on the YouTube channel too. The party uses also X and Facebook.

The party relies on traditional decision-making processes that require the personal presence of delegates. Elections to statutory bodies, including the party chair, are held by attending the local party headquarters and casting a ballot in a traditional ballot box.

3.7. The Law and Justice

The Law and Justice is the party with the oldest electorate, aged on average over 50 and over, whom it reaches through television and other traditional media, not social media. Furthermore, party leader Jarosław Kaczyński does not use social media himself, and there are even doubts as to whether he uses the internet at all. Therefore in August 2025 the party created its own smartphone app named White and Red (*Biało-Czerwona*, the colours of the Polish flag) to engage young people in its activities, to 'modernize the party' and 'strengthen mobilization before the elections'. What appears innovative and modern at first glance turns out to be unengaging. After logging in, the app welcomes users with a collection of 'the latest information and materials to help support the white-and-red team'. This includes links to social media posts (X, TikTok, YouTube, Facebook, Instagram) from the PiS party's profiles and those of politicians associated with it. We find exactly the same content on TikTok, Instagram and YouTube. The Biało-Czerwona app can hardly even be called an app, as it is a collection of several statements by the party leader, edited by the press office, and a partially functioning aggregator of content from party social media. The app does not have any original features, such as a discussion forum or the ability to send messages to politicians. It is hard to resist the impression that it serves only to collect users' personal data.

The Law and Justice has a fairly traditional and static website. Since autumn 2024, when the State Electoral Commission decided to reduce state subsidies for the party due to irregularities in the financing of the 2023 parliamentary campaign, the most conspicuous section on the website is the one entitled 'Support us'. However, it is not possible to make a payment through a dedicated gateway; only information on the conditions that must be met and how to make a traditional bank transfer is provided. It is also not possible to join the party via the website, although it is possible to leave contact details and declare an interest in starting the membership procedure.

The party does not use any digital tools to increase members' sense of influence on party decisions, and is based on traditional decision-making processes that require the personal presence of selected members at meetings of statutory bodies.

Table 3. Comparison of the digitalization of Polish political parties.

	R	K	PL2050	PSL	PO	NL	PiS
Electoral pillar							
online voting (party leadership)	Y	N	Y	N	N	N	N
online voting (candidates)	N	N	N	N	N	N	N
online voting (party bodies)	Y	N	N	N	N	N	N
Deliberative pillar							
deliberative online platforms	Y	N	N	N	N	N	N
other deliberative online initiatives	Y	N	Y	N	N	N	N
party congresses digitalization	N	N	N	N	N	N	N
Participatory pillar							
online consultations	Y	N	N	Y	Y	N	N
online membership	N	Y	N	N	N	N	N
digital activities for electoral campaign	Y	N	N	N	N	N	N
Resources pillar							
online fee payment	N	Y	N	Y	N	N	N
online crowdfunding/ donations	Y	Y	Y	Y	N	N	N
official online store	N	N	N	N	N	N	N
Communication pillar							
party website	Y	Y	Y	Y	Y	Y	Y

Social Networking Sites (SNS), Mobile Instant Messaging Services (MIMS)	Y	Y	Y	Y	Y	Y	Y
other forms of online communication	Y	Y	Y	N	Y	Y	Y
Score	**10**	**6**	**6**	**5**	**4**	**3**	**3**

Y – yes

N – no

Source: Author's elaboration

Conclusions

The evidence from the analysis of the Polish political parties confirms that digitalization is more advanced in the external pillars that directly link parties with voters (communication and resources) than in the dimensions related to internal party procedures. This is consistent with the results obtained in the DIGIPART project, whose methodology was used as an analytical framework. The analysis partly confirms the intuitive expectation that being a new party has a positive impact on the use of digital tools, although it does not determine whether digitalization affects all dimensions equally. Of the three youngest parties analysed here, only the Together Party stands out in its use of online platforms both in external communications and in resource acquisition, as well as within the organization in the electoral, deliberative and participatory pillars. In its early stages, the Poland 2050 also showed openness to innovations that affect the participatory and deliberative pillars of internal organization, but this was not a lasting trend. The Confederation, on the other hand, focused on building a base of supporters and voters rather than party activists, developing a vertical online linkage between the leader, voters and supporters, and does not invest in digital intra-party democracy procedures.

An analysis of the Polish case also shows that even older, well-established organizations, such as the Polish People's Party, are trying to replace their existing, tried-and-tested methods with new technologies and are demonstrating their ability to adapt to change. Therefore, it is not the age of the party that is the most important variable. It seems that parties with a high level of internal democracy are more open to technological progress and more willing to embrace digital conveniences, supplementing them with more traditional methods. On the other hand, if a party does not have mechanisms of participation or deliberation in its DNA, and the process of internal party elections is intended to confirm the will of the leadership or, to put it bluntly, the will of a single leader (such as in the case of the Law and Justice), then it sees no need for internal digitalization. The Polish case also shows that a party's dis-

tance from the centre on the right–left axis is an indicator (though not a predictor) of the level of party digitalization.

The next step in research could be to determine the relationship between the level of digitalization of political parties and their organizational culture. To avoid speculation on this subject, qualitative interviews with the parties' leaderships should be conducted. Another research recommendation is to conduct quantitative surveys among members, supporters and voters of individual parties in order to assess the effectiveness of the external dimension of party digitalization from the perspective of its target audience. This would allow the question of whether digitalization translates into greater political engagement among citizens to be answered.

REFERENCES

Barberà, O., Barrio, A., & Rodríguez-Teruel, J. (2019). New parties' linkages with external groups and civil society in Spain: A preliminary assessment. *Mediterranean Politics*, *24*(5), 646–664.

Barnea, S., & Rahat, G. (2007). Reforming candidate selection methods: A three-level approach. *Party Politics*, *13*(3), 375–394.

Bennett, W. L., & Segerberg, A. (2013). *The logic of connective action: Digital media and the personalization of contentious politics*. Cambridge University Press.

Correa, P., Rodríguez-Teruel, J., & Barberà, O. (2024). The use of party websites for political information among Spanish party activists. *Party Politics*, *31*(2), 239–250.

Cross, W. P., & Gauja, A. (2019). Selecting party leaders, reform processes and methods: Examining the Australian and New Zealand Labour parties. *International Political Science Review*, *42*(2), 261–276.

Cross, W. P., & Katz, R. S. (2013). *The challenges of intra-party democracy*. Oxford University Press.

Datts, M., & Gerl, K. (2024). Intra-party communication in the digital era: An empirical case study of party delegates from the German Greens. *German Politics*, *33*(1), 155–177.

Deseriis, M. (2020). Digital movement parties: A comparative analysis of the technopolitical cultures and the participation platforms of the Movimento 5 Stelle and the Piratenpartei. *Information, Communication & Society*, *23*(12), 1770–1786.

Dommett, K., & Temple, L. (2018). Digital campaigning: The rise of Facebook and satellite campaigns. *Parliamentary Affairs*, *71*(1), 189–202.

Gerbaudo, P. (2019). *The digital party: Political organisation and online democracy*. Pluto Press.

Gerbaudo, P. (2021). Are digital parties more democratic than traditional parties? Evaluating Podemos and Movimento 5 Stelle's online decision-making platforms. *Party Politics*, *27*(4), 730–742.

Gibson, R., & Ward, S. (2009). Parties in the digital age. *Representation*, *45*(1), 87–100.

Gibson, R., Greffet, F., & Cantijoch, M. (2018). Friend or foe? Digital technologies and the changing nature of party membership. In K. Koc-Michalska, G. Darren, & D. G. Lilleker (Eds.), *Digital politics: Mobilization, engagement and participation* (pp. 89–111). Routledge.

Giovanola, B. (2023). Justice, emotions, socially disruptive technologies. *Critical Review of International Social and Political Philosophy*, *26*(1), 104–119.

González-Cacheda, B., & Cancela Outeda, C. (2024). Digitalisation and political parties in Europe. *Party Politics*, *31*(3), 488–498.

Invernizzi-Accetti, C., & Wolkenstein, F. (2017). The crisis of party democracy, cognitive mobilization, and the case for making parties more deliberative. *American Political Science Review*, *111*(1), 97–109.

Jääsaari, J., & Šárovec, D. (2021). Pirate parties: The original digital party family. In O. Barberà, G. Sandri, P. Correa, & J. Rodríguez-Teruel (Eds.), *Digital parties: The challenges of online organisation and participation* (pp. 205–226). Springer.

Jacuński, M. (2022). Proces digitalizacji partii politycznych – w kierunku interdyscyplinarności badań. *Wrocławskie Studia Politologiczne*, *31*, 107–116.

Jędral, P. (2025, 6 June). Tysiące młodych zapisują się do Razem i Lewicy. Czy to początek nowego fenomenu? *Kultura Liberalna*, *22*. https://kulturaliberalna.pl/2025/06/06/jedral-tysiace-mlodych-zapisuje-sie-do-razem-i-lewicy-czy-to-poczatek-nowego-fenomenu/

Mair, P. (2013). *Ruling the void. The Hollowing-out of Western Democracies*. Verso.

Margetts, H. (2006). Cyber parties. In R. S. Katz, & W. J. Crotty (Eds.), *Handbook of party politics* (pp. 528–535). Sage Publications.

Oross, D., & Tap, P. (2023). Moving online: Political parties and the internal use of digital tools in Hungary. *European Societies*, *25*(2), 346–370.

Pacześniak, A. (2023). The anti-elitist strategy of political parties as a populist tool to (re)gain electoral support. *Journal of Contemporary European Studies*, *32*(4), 1021–1032.

Pacześniak, A., & Wincławska, M. (2017). Czy współczesne partie potrzebują jeszcze członków? Wnioski z badań empirycznych w polskich partiach politycznych. *Political Preferences*, *17*, 7–26.

Pedersen, K., & Saglie, J. (2005). New technology in ageing parties. Internet use in Danish and Norwegian parties. *Party Politics*, *11*(3), 359–377.

Peña, A. M. (2021). Activist parties and hybrid party behaviours: A typological reassessment of partisan mobilisation. *Political Studies Review*, *19*(4), 637–655.

Peña, A. M., & Gold, T. (2023). The party-on-the-net: The digital face of partisan organization and activism. *Information, Communication & Society*, *26*(16), 3257–3274.

Poguntke, T., Scarrow, S., & Webb, P. (2016). Party rules, party resources and the politics of parliamentary democracies: How parties organize in the 21st century. *Party Politics*, *22*(6), 661–678.

Poguntke, T., Scarrow, S., & Webb, P. (2021). Democracy, deliberation and social distancing in the pandemic: Adaptive strategies in legislatures and political parties. *Zeitschrift für Parteienwissenschaften*, *1*, 15–21.

Ponce, A., & Scarrow, S. (2016). Which members? Using cross-national surveys to study party membership. *Party Politics*, *22*(6), 679–690.

Rek, M. (2024). E-democracy in the EU. In D. Troitiño (Ed.), *E-governance in the European Union: Strategies, tools, and implementation* (pp. 103–115). Springer Nature Switzerland.

Sandri, G., Lupato, F. G., Meloni, M., von Nostitz, F., & Barberà, O. (2025). Mapping the digitalisation of European political parties. *Information, Communication & Society*, *28*(10), 1757–1778.

Scarrow, S., & Gezgor, B. (2010). Declining memberships, changing members? European political party members in a new era. *Party Politics*, *16*(6), 823–843.

Scarrow, S. E., Webb, P. D., & Poguntke, T. (2017). *Organizing political parties: Representation, participation, and power*. Oxford University Press.

Sejm of Poland. (n.d.) *Kluby i koła*. Retrieved 7 January 2026, from https://www.sejm.gov.pl/Sejm10.nsf/kluby.xsp

Troitiño, D. R. (2022). The European Union facing the 21st century: The digital revolution. *TalTech Journal of European Studies*, *12*(1), 60–78.

Ziegler, S., Borucki, I., & Weissenbach, K. (2024). The digital transformation of party membership: How party members perceive online participation and adapt to it under pandemic circumstances. *Party Politics*, *31*(2), 251–264.

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

sciendo

DOI: 10.15290/bsp.2026.31.01.17

Received: 30.06.2025
Accepted: 08.01.2026

Aleksandra Klich
University of Szczecin, Poland
aleksandra.klich@usz.edu.pl
ORCID ID: 0000–0002–2931–712X

Katarzyna Syroka-Marczewska
University of Warsaw, Poland
k.syroka-marczewska@wpia.uw.edu.pl
ORCID ID: 0000–0003–4177–6721

Neringa Gaubienė
Vilnius University, Lithuania
neringa.gaubiene@tf.vu.lt
ORCID ID: 0009–0002–6756–2246

Kristina Pranevičienė
Vilnius University, Lithuania
kristina.praneviciene@gmail.com
ORCID ID: 0009–0007–9117–635X

Judicial Reform in the Era of Digital Democracy from the Perspective of Ensuring the Rule of Law: The Perspective from Poland and Lithuania

Abstract: In this article, we explore the complex challenges and opportunities arising from the digital transformation of the judiciary in the context of modern democratic societies, with a particular focus on Poland and Lithuania. As digital tools increasingly shape how justice is administered, ensuring the rule of law, transparency, and fair trials remains a central concern. We analyse the legal, institutional, and technological aspects of judicial reforms, including the use of remote hearings, algorithmic decision-making, online access to court services, and the risks of digital exclusion. Drawing on European standards, we highlight the need to strike a careful balance between innovation and fundamental rights. By examining recent legislative initiatives, court practices, and comparative insights from both countries,

this article contributes to the broader discourse on the legitimacy, efficiency, and accountability of digital justice systems in a democratic setting.

Keywords: e-democracy, e-justice, judicial reform, access to justice, fair trial, digital justice

Introduction

When the impact of e-democracy on the justice system is analysed, it is essential to emphasize that the widespread adoption of the internet has led to the development of new organizational and technical platforms for the democratic process, paving the way for so-called 'digital democracy' (Pianini & Omicini, 2019, p. 84). The popularization of other digital technologies, such as big data and artificial intelligence, has contributed to the world entering an era characterized by the transformation of information into valuable yet highly advanced resources (Horváth et al., 2025, p. 107). The digital revolution is currently bringing about fundamental changes in many areas. Technologies that only existed in theory a few decades ago are now ubiquitous and shape the way we communicate, work, learn, and make decisions, which also affects the structure of a democratic state governed by the rule of law and the functioning of its justice system. From the perspective of such states, people who are digitally excluded or at risk of exclusion must not be overlooked. In other words, in the era of digital democracy, the use of technological solutions offers on the one hand significant potential for increasing citizens' access to decision-making processes and public institutions. On the other hand, however, this development brings with it a very real risk of digital exclusion, which may result in the marginalization of groups that were already on the sidelines of social and political life.

Attention should also be paid to the principle of privacy, which is key from the perspective of the rule of law. It is seen as a foundation of democracy because without it, there is an increased risk of individuals using their power to influence others (Janssen & van den Hoven, 2015). Digital democracy consumes large amounts of data, and public services that are more targeted, tailored to needs, cheaper, and faster actually require intensive data use (Squeo, 2023, p. 61). For this reason, the design and implementation of new tools requires the creation of an appropriate regulatory framework; otherwise, we will face a serious threat to individual privacy.

The topic of this article is related to the need to analyse the relationship between digital transformation, judicial reform, and the maintenance of (or threat to) the rule of law. At the heart of this analysis is the question of how judicial reforms carried out in the era of digital democracy affect the implementation of the rule of law. The main objective of the study is to identify the risks and benefits associated with the digitization and computerization of the justice system, as well as to assess whether and to what extent the technologies being implemented, such as automation, remote access tools, and decision-support systems, remain consistent with constitutional guarantees of a fair trial, the independence of courts, and the transparency of public institu-

tions. The analysis focuses on assessing the compliance of digital solutions with the fundamental principles of a democratic state governed by the rule of law and on comparing the models adopted in countries whose legal systems and judicial reforms we examine from an internal perspective, i.e. Poland and Lithuania.

This article aims to examine several interrelated hypotheses concerning the digital transformation of the judiciary and its implications for the rule of law. First, it is assumed that the ongoing digitalization of judicial processes may strengthen the rule of law only to the extent that transparency and procedural safeguards are effectively maintained. Second, digital innovation in the courts can enhance citizens' access to justice and their participatory role, provided that both technological constraints and users' diverse needs are adequately addressed. Third, the broader process of judicial reform undertaken in the era of digital democracy may enhance the legitimacy of the justice system. Nevertheless, poorly designed or politically driven digital measures may, conversely, endanger judicial independence and the right to a fair trial. Furthermore, the study assumes that it is possible to achieve a balance between efficiency and fairness; digital tools can promote transparency and uphold procedural rights if implemented with due respect for the roles of all participants in judicial proceedings. Finally, the research acknowledges that technological change is not merely technical but transformative, as emerging technologies reshape the way legal and political decisions are made. For this reason, any sustainable digital transformation of justice must begin with a thorough assessment of institutional capacities and systemic needs.

This choice is justified by the availability of sources and knowledge of local institutional conditions, as well as the dynamic nature of reforms in the area of digitization and computerization of the justice system in both countries. This approach enables the analysed cases to be situated within a broader comparative legal context, even if these references are not the subject of in-depth case studies. In particular, the elements of the reforms aimed at increasing the efficiency of the courts and access to justice, which may at the same time pose a risk of restricting the procedural rights of parties to proceedings, were subject to verification. Richard E. Susskind (2019, p. 368) has examined the transformative potential of online courts in enhancing access to justice. In this context, it was assumed that digital technologies can strengthen the rule of law, provided that they are implemented transparently, with respect for procedural guarantees and judicial and civic control mechanisms. Alternatively, it is assumed that the improper implementation of digital tools – especially without public consultation and without a clear legal framework – may lead to the erosion of fundamental standards for fair trials. This article is based on a comparative and dogmatic legal analysis, taking into account standards developed by international institutions (including the Council of Europe and the European Union), as well as the practices of Poland and Lithuania in implementing digitalization models for the justice system. The Lithuanian experience is significant, as it is more advanced in terms of technology and institutions and has been a considerable

inspiration for assessing the opportunities and threats associated with the digital transformation of the justice system in Poland.

1. The role of digital democracy

The impact of information and communication technologies on the relationship between the state and its citizens can be described using terms such as internet democracy, digital democracy, cyberdemocracy, virtual democracy, or, more commonly, electronic democracy (Musiał-Karg & Kapsa, 2020, p. 145). Digital democracy, which is evolving in response to shifting communication and technological conditions within societies, refers to a radically new form of democratic practice modified by new information technologies. Regardless of the name or scope of the definition, a common feature of these concepts is the belief that new technologies (which provide an interactive dimension, faster information transfer, and feedback) make it possible to influence democratic mechanisms (Friedland, 1996; Hagen, 1997). They are understood as a form of action by the authorities, whereby public authorities and public administration bodies are required to counteract any trends that are detrimental to national security. As a result, government administration and local government bodies can provide more efficient and practical assistance in crises related to information and electronic communication technologies (ICT) infrastructure if third-sector organizations offer professional support (Chałubińska-Jentkiewicz, 2019, p. 292). The use of digital technologies also broadens and deepens civic participation, as well as increasing the transparency of public life. In this model, citizens not only vote but can also take action in public consultations on an ongoing and rapid basis, express their opinions online, submit electronic petitions, participate in digital participatory budgeting, and even co-create laws through legislative crowdsourcing tools. Both models of democracy, traditional and digital, are based on a common political principle that decisions should be made transparently and that individual rights must be protected.

However, the tools and scope of civic activity are what differentiate the two models. The role of ICT boils down to verifying whether e-democracy (digital democracy) encompasses only the aspect related to the provision of a specific public service by public administration bodies. In this context, it should be verified whether this provision is based solely on management (e-government in the narrow sense). In such a situation, mutual interaction involves the performance of a public task for the benefit of the individual and, on the other hand, the performance of a duty by the citizen for the benefit of a specific authority. The second issue that should be considered is whether e-democracy refers not only to the distributive function of administration, but also includes elements of public participation in public life (e.g. the right of access to public information, e-consultations, e-petitions, e-voting). Both issues play

a crucial role in shaping digital democracy, and must work together to ensure that changes in policy and strategy for the development of electronic communications in EU Member States are practical and efficient.

Polish literature on the subject expresses the view that electronic administration is synonymous with electronic democracy (Skoczylas, 2023, pp. 327–328). This is justified by the fact that the development of electronic administration procedures is intended not only to improve the efficiency of public institutions, but also, and above all, to have a substantial impact on the model of modern democracy. In this view, ICTs are a tool that transforms the state to a much greater extent; this approach prevails over the view that ICT is a technological innovation that allows for the streamlining of bureaucracy (Porębski, 2013, pp. 61–62). This means that it should be efficient, streamline administration, and increase the effectiveness of interactions between citizens and the state. There is no doubt that digital democracy removes many barriers, including temporal, geographical, and organizational ones. At the same time, it enables not only faster, but also broader access to decision-making processes. Due to the use of modern technological solutions, its application imposes numerous obligations on state authorities, including the need to ensure cybersecurity, personal data protection, the transparency of algorithms, counteracting disinformation, and, most importantly, preventing digital exclusion.

An essential aspect of e-democracy is its impact on the relationship between citizens and the state. In the classical view, democracy is based on trust in institutions and their representatives. Digital democracy, on the other hand, is compelled to consider non-human factors, namely technology, algorithms, and automated decision-making systems, in civic processes. While the classic model of democracy relies on modern technologies to support its everyday functioning, in the case of e-democracy it seems reasonable to assume that technology is co-shaping it. This not only applies to communication and logistics, but also covers a much wider range of areas. In this context, the fundamental challenge for digital democracy is to ensure that non-human factors are transparent, controllable, and consistent with democratic values. It is unacceptable to shape e-democracy in such a way that modern tools contradict the idea of a democratic state governed by the rule of law. Access to digital public space enables access to diverse content, and this in turn ensures pluralism, fosters open public debate, and promotes effective participation in democracy. The consequence is civic engagement in the digital space (Małecka-Łyszczek, 2024, pp. 15–20 Recital 18 of Decision (EU) 2022/2081 of the European Parliament and the European Council clearly emphasizes that democracy and key public services depend significantly on digital technologies; at the same time, it points out that every citizen and business should be able to interact digitally with public administrations. In light of the wording of Recital 18, it can be inferred that universal access to digital interaction is the foundation of effective digital democracy. This should be understood as the basis for equal access to services, regardless of place of residence or social status.

Furthermore, digital services must be designed with the needs of users, citizens, and businesses in mind, and should be transparent, intuitive, easy to use, and easy to understand. This builds trust in e-democracy. A high-quality digital environment is also essential, which should be directly linked to the reliability, efficiency, and personalization of services. Citizens should feel that systems are designed to help them, not to make their lives more difficult. Achieving this goal is directly linked to the need for investment in infrastructure and software that can meet these requirements. Digital democracy aims to digitize all key services, especially those related to significant events in people's lives (e.g. birth, education, employment, starting a business). The EU legislation pays particular attention to electronic medical records, which perfectly reflects the potential for improving quality of life through digitization. While classical democracy is based on trust in institutions and their representatives, digital democracy assumes more frequent, direct, and dynamic interactions, and is associated with control over public administration through the use of modern tools (Viegas et al., 2022, p. 342). Public institutions must be able to respond quickly to social signals, open up to data, and enable dialogue and co-management, which requires not only new tools, but also a change in administrative and legal culture. Both models should complement each other: digital democracy does not replace classical democracy but can strengthen and update it, provided that it is developed in an inclusive, responsible, and lawful manner. It is important to note that despite the drive towards digitalization, people who for various reasons (e.g. lack of internet access, lack of digital skills, disability, reluctance, exclusion or being at risk of exclusion) are unable to use online services or do not want to exercise their rights in this way cannot be excluded. Consequently, services should be designed to ensure access for all while providing alternative access channels (e.g. support in using IT systems or offline access).

Also noteworthy is the wording of Recital 19 of the Decision (EU) 2022/2081, in which the legislation deepens the perspective of digital democracy, going beyond mere access to services and focusing on its broader, transformative social effects. Digital technologies should be seen as a catalyst for positive social change; they are not an end in themselves but should be used as a tool to achieve broader social effects. This means that, from the perspective of e-democracy, digitization should serve to improve the daily lives and well-being of citizens. This applies to faster online services, and also has a tangible impact on the quality of life, which can be related to better access to information or education, and to the possibility of more active participation in public life. Designing solutions based on this principle will help to emphasize the humanistic and social dimension of digital democracy. In this regard, digital transformation is directly linked to democratic values and is a fundamental principle of digital democracy, as digital technologies must support, not undermine, the basic pillars of a democratic state. This means that digital technologies can contribute to more effective, transparent, and accountable governance.

To sum up, digital democracy should be recognized not only as a technology, but above all as a philosophy of state governance that continues to place citizens at the centre. Its goal is to facilitate everyday life, increase the availability of services, and strengthen trust in public administration through digital tools. It cannot be implemented in a way that marginalizes the need for inclusiveness and security; its success depends on whether it serves to strengthen democratic values, promote good governance, ensure social inclusiveness, and bring about real improvements in the quality of life of citizens.

2. Challenges for the judiciary in the digital age

As European judiciaries undergo rapid digitization, courts face opportunities and challenges. On the one hand, digital tools promise greater efficiency and accessibility: the EU notes the 'enormous potential' for digital and AI systems to improve access to justice for all (European Commission, 2025). There is no doubt that, from a technical perspective, AI systems will generally outperform humans in tasks that require precision, repeatability, and the processing of large amounts of data within a short timeframe. However, this does not mean that they can be guaranteed to perform the tasks entrusted to them in a manner that can be considered socially appropriate (Rejmaniak, 2021, p. 26). On the other hand, these innovations raise serious questions about how to uphold fundamental rights and the rule of law in an online environment. This section examines the key challenges facing Europe's courts in the digital age, including access to justice, data protection, judicial independence, and the application of AI in adjudication.

Moving court processes online can inadvertently create 'digital divides' that undermine equal access to justice (European Commission, 2025). To promote a fair and balanced justice landscape across Europe, it is essential to reduce any such divides. Not all citizens have the necessary internet access, equipment, or digital literacy to engage with e-justice services: nearly half of Europeans lack basic digital skills (European Commission, 2025), a statistic that highlights the scale of potential exclusion. Vulnerable groups – such as older people, low-income individuals, or rural populations – are at particular risk of digital exclusion if paper-based or in-person alternatives are unavailable. The European E-Justice Strategy (2024–2028) explicitly calls for bridging this divide, warning that unequal access to digital justice 'creates inequality in access to justice' overall, and can become 'a potential source of exclusion' (European Commission, 2025). Courts must therefore pursue a people-centric digital transformation: services should be user-friendly and inclusive by design, with accommodations for those unable or unwilling to use technology, and, importantly, non-digital channels must be maintained as a safeguard against potential disruptions. For example, even as filings and hearings move

online, many jurisdictions continue to accept paper submissions or provide physical kiosks and assistance for self-represented litigants.

In 2018 the Law of the Republic of Lithuania on Electronic Identification and Trust Services for Electronic Transactions entered into force. Its purpose is to create a legal basis for the effective operation of electronic identification and the market of trust services in the Republic of Lithuania, in order to ensure the best possible protection of the interests of the users of these services. The Law regulates the legal effect of electronic signatures, electronic seals, electronic time stamps and trust services, as well as the obligations of trust service providers and users.It also governs the conditions and procedures for the suspension and revocation of qualified certificates for electronic signatures, electronic seals, and website authentication. Furthermore, it provides for the supervision of trust service providers in matters not regulated by Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market (OJ 2014 L 257, p. 73) and by implementing acts adopted by the European Commission on that basis.The Law additionally regulates electronic identification and designates the competent authorities responsible for trust services.

As court proceedings and records migrate to digital platforms, privacy and data protection have become one of the biggest concerns. Judicial systems handle vast amounts of sensitive personal data (from case files to recordings of hearings), raising the stakes for cybersecurity and GDPR compliance. European courts are obliged to safeguard the confidentiality and integrity of judicial data at the same level as in traditional settings. The Council of Europe's guidelines on cyberjustice emphasize that data protection principles, along with data quality and security, 'shall be ensured' in digitalized judicial processes (CEPEJ, 2021). This means e-filing systems must employ encryption and authentication; case management databases require strict access controls and audit trails, and any sharing of data across agencies or borders must respect privacy laws. An additional challenge is reconciling the ideal of open justice (the publishing of decisions for transparency) with the need for personal privacy. Likewise, courts must carefully manage audio and video recordings of hearings, preventing unauthorized dissemination and ensuring that any live streams do not compromise the confidentiality of witnesses or the right to a fair trial. The EU's e-justice strategy emphasizes respect for fundamental rights in all digital initiatives, and highlights risks that could erode public trust, such as cybersecurity breaches or personal data leaks. In response, judiciaries are increasingly adopting a 'data protection by design' approach, where privacy considerations are built into new IT systems from the outset (CEPEJ, 2021).

The digitization of justice also poses other dangers to judicial autonomy and independence. One concern is that digital case management systems and algorithms might shift control of judicial decision-making processes away from judges (Limantė et al., 2025, p. 8). Another concern is the role of private tech companies that provide

court IT infrastructure, from cloud services to videoconferencing platforms; heavy dependence on external vendors, especially those that control critical data or algorithms, could indirectly impact judicial independence (Castets-Renard & Eynard, 2023). The European Network of Councils for the Judiciary (ENCJ, 2017) has cautioned that judiciaries must be closely involved in developing and governing e-justice tools: judges and court administrators, not just ministries or IT firms, should set the requirements to ensure that judicial values (such as independence and fairness) are embedded in the technology.

A related concern is the use of performance analytics on judges' work. Digital systems enable easy tracking of how fast judges resolve cases or how often their rulings are upheld. While such data can improve efficiency, there is a risk that it could be misused to pressure judges or undermine their decisional independence. Any evaluation criteria must therefore be carefully balanced so that judges feel free to decide cases on the merits, not to satisfy metrics. Ultimately, maintaining judicial independence in the digital era requires transparency, oversight, and a reaffirmation that technology will remain a tool subordinate to human adjudication, not a replacement for it. Therefore digital literacy, especially literacy in artificial intelligence, is essential for judges (Limantė et al., 2025).

Perhaps the most complex challenge is the rise of artificial intelligence in court operations and even in decision-making. Justice systems across Europe are increasingly exploring the use of AI technologies through various pilot initiatives (Mukhtar & Siddiqah, 2025). They offer excellent benefits: speeding up document review, suggesting relevant precedents, and even assisting in drafting decisions. However, if not adequately regulated, the use of AI poses significant risks to the principles of fairness and the rule of law. While the EU Artificial Intelligence Act (Regulation (EU) 2024/1689) has brought greater clarity regarding the use of artificial intelligence in judicial contexts, the absence of formally adopted standards across Europe leaves uncertainty as to which AI systems are suitable for deployment in courts. Given the potential impact on individual rights and judicial independence, AI applications in judicial proceedings are most likely to fall under the category of high-risk systems within the meaning of the EU AI Act.

One primary concern is algorithmic bias. AI tools trained on past judicial data might uphold historical biases or discrimination, thereby undermining the right to an equal and fair trial. The EU has explicitly warned that 'unconscious discrimination due to biased algorithms or datasets' (European Commission, 2025) is a new challenge brought by digitization. A related issue is the 'black-box' opacity of many AI models; if a judge or litigant cannot understand how an algorithm arrived at a recommendation, this conflicts with the transparency required of judicial reasoning (Socol de la Osa & Remolina, 2024, p. e59). Generative AI tools, such as large language models capable of drafting legal texts, pose a potential threat to judicial independence by introducing the risk of undue influence on legal reasoning (Socol de la

Osa & Remolina, 2024, p. e59). Judges using these tools must remain the ultimate arbiters, consciously verifying and correcting AI outputs. European bodies have begun to address these risks: the Council of Europe's Ethical Charter on the Use of Artificial Intelligence in Judicial Systems (CEPEJ, 2018) and the EU Artificial Intelligence Act establish key guiding principles, including the requirement that AI systems respect fundamental rights, operate without bias, ensure transparency, and remain subject to human oversight. However, significant challenges persist, particularly concerning the practical implementation and enforcement of these principles across jurisdictions. This implies that AI should serve a strictly supportive function within judicial proceedings, such as assisting in the organization and analysis of information. At the same time, the ultimate responsibility for decision-making must remain exclusively with judges. In the future, ongoing judicial AI literacy training will be essential to ensure that the benefits of such technologies are realized without the principles of fairness, accountability, and public confidence in the justice system being compromised.

3. Digital technologies as an opportunity for the legal system and the judiciary

Applying the above considerations to the issue of law and the judiciary, it should be noted that modern technological solutions have a profound impact on the functioning of the justice system in its broadest sense. Digital transformation affects not only proceedings but also institutional structures, the relationships between actors, and the implementation of fundamental rights. It is first necessary to identify the groups of participants in this system who are directly affected by the digital transformation. This concerns four categories of relationships: a) citizen–judicial authority; b) participant in proceedings or their professional representative–judicial authority; c) judicial authority–administrative staff; d) government/Minister of Justice–judicial authorities. A common feature of all relationship models is that electronic interactions can strengthen the position of citizens on three primary levels: a) direct participation in political life; b) accessibility, referring both to easy access to public government information and to access to online services provided by e-government; c) the ability to monitor and influence government decisions (Ronchi, 2019, p. 64). From the perspective of the justice system, digital tools enhance citizens' ability to access information, reduce barriers to entry, and reinforce their sense of agency.

When analysing the above levels from the perspective of the justice system, it is worth noting that although citizens do not participate directly in adjudication (except for lay judges, for example), digital tools enable them to actively use IT tools, which strengthens their sense of agency and reduces the barrier to entry into the justice system. Accessibility should be understood as referring to the transparency and accessibility of digital justice. The digitalization of the judiciary enhances access to rulings,

reasoning, court schedules, and online services. In the area of oversight and influence, such as citizen oversight of the judiciary, electronic interactions enable public monitoring of court activities based on publicly available data, thereby increasing accountability and transparency. In this respect, citizens not only gain greater knowledge, but also the ability to exert constructive pressure on institutions to improve the quality of justice.

In the first group of relationships, i.e. between citizens and judicial authorities (the so-called citizen level), it is essential that, from the citizen's perspective, digitization enables greater access to legal information, including legal acts, case law, and public registers. Polish examples include the Portal of Common Court Judgments (https://orzeczenia.ms.gov.pl/), the Internet System of Legal Acts (https://isap.sejm.gov.pl/), and the Central Database of Administrative Court Judgments (https://orzeczenia.nsa.gov.pl/cbo/query). The solutions introduced in this area serve as the foundation for an informed civil society and the enforcement of rights, while also increasing the transparency of the legal system. They contribute to the implementation of Article 45 of the Constitution of the Republic of Poland (the right to a fair and public hearing) and Article 6 of the European Convention on Human Rights (which guarantees access to justice and transparency of proceedings). They also indirectly contribute to building and raising legal awareness among the public.

Digital accessibility policies also mitigate the risk of digital exclusion by ensuring that public legal information remains free and open. In addition, digital platforms used by public administrations contribute to increasing citizens' participation in legislative processes, e.g. by enabling them to submit comments and opinions on draft legislation. These solutions strengthen the legitimacy of legislative processes, supports the democratic legitimacy of lawmaking, and corresponds with the principles of open government. E-democracy also has a direct impact on the expansion of the catalogue of fundamental rights and freedoms, to include those related to the use of modern technological solutions known as digital rights (e.g. the right to privacy on the internet or the right to be forgotten). These rights are now recognized under the GDPR (European Parliament, 2016) and Article 8 of the Charter of Fundamental Rights of the EU (European Union, 2000). The protection of these rights is becoming a key element of digital democracy. Solutions that introduce the digitization of processes (e.g. in public procurement) are crucial for the legal system and the effective implementation of the rights. In this case, good governance is secured by minimizing the risk of interference aims at achieving individual benefits.

When analysing manifestations of e-democracy in the relationships between participants in proceedings, their representatives, and judicial authorities (e.g. courts or prosecutors), particular attention should be paid to the impact of ICT systems on procedural transparency. Electronic court schedules, access to case files, or information about cases using dedicated ICT systems, and sometimes even the possibility of initiating court proceedings electronically, are now standard in modern society. The delivery of procedural documents to professional representatives via a dedicated

platform reduces the need for personal visits to court, increasing the transparency and comprehensibility of the judicial process. These solutions are grounded in Articles 148[1] and 151 §2 of the Polish Code of Civil Procedure, which regulate remote hearings and electronic submissions.

The modernization of the justice system must not result in anyone being deprived of the right to a fair trial. . This reflects the guarantees of Article 47 of the Charter of Fundamental Rights of the EU and the principle of equality of arms. These solutions not only build public trust, but also enable social control. Digital technologies also reduce geographical, financial, and physical barriers to accessing courts, e.g. by allowing participation in so-called remote hearings or the examination of witnesses or experts via videoconferencing. This aligns with the Council of Europe's European Ethical Charter on the use of Artificial Intelligence in judicial systems (CEPEJ, 2018), which promotes the development of AI tools that enhance accessibility, efficiency and fairness in judicial proceedings. This is particularly important for people living in remote areas, older people, people with disabilities, or those unable to appear in person due to increased professional responsibilities (which is characteristic of court experts who are specialists in narrow fields of science). In this respect, the burden of physical appearance in court is transferred to the digital sphere, which not only removes geographical and financial barriers, but also has a positive impact psychologically, eliminating or reducing stress, for example. A direct effect of these solutions is also the acceleration of court proceedings, which is particularly evident in the elimination (or reduction) of paper files, the introduction of electronic document circulation, and the delivery of procedural documents using an ICT system. This not only speeds up proceedings, but also reduces costs and minimizes the risk of documents getting lost.

Contemporary law increasingly utilizes LegalTech and RegTech tools to support the processes of analysing, applying, and enforcing the law (Szostek, 2021a, p. 45; Szostek, 2021b, pp. 3–10). A significant qualitative change can be observed in the internal functioning of judicial authorities. Case management systems enable more effective tracking of case progress, deadline management, task allocation, and verification of task completion (Mummalaneni & Challa, 2024, p. 158). These systems contribute to the principle of accountability and transparency, improving oversight within judicial administration, and improve access to all necessary documents and information in one place. The digitization of files, either in whole or in part (e.g. in the area of procedural documents, as currently observed in Polish civil proceedings), increases the accessibility of documents and enables them to be accessed from anywhere. Internal transparency is also essential. The introduction of appropriate tools ensures easier control over case processing, which in turn has a positive impact on accountability. The use of artificial intelligence, particularly decision-support tools, can also assist authorities in data analysis, identifying similar cases and preparing draft decisions. This offers new opportunities but also raises questions about transparency and human oversight. The Council of Europe's Ethical Charter on the Use of

Artificial Intelligence in Judicial Systems (2018) stresses that AI must remain subordinate to human decision-making and cannot replace judicial discretion.

In the relationship between the judiciary and the government or the Minister of Justice, it is important to distinguish those activities in which ICT provides large amounts of data on the functioning of courts (e.g. the number of cases, the duration of proceedings, or the workload of individual courts). This has a positive impact on the ability to monitor the effectiveness of the judiciary, identify problems, and plan strategically. However, the collection and use of such data must respect the constitutional principle of judicial independence, enshrined in Articles 173–178 of the Constitution of the Republic of Poland, and must prevent any executive interference. It is also essential that IT systems do not allow the executive branch to interfere with the independence and impartiality of the judiciary, which is the foundation of the judicial system's functioning.

ICT in the judiciary cannot be viewed solely in terms of technical modernization. Digitalization represents a structural transformation that requires not only technical capacity, but also ethical awareness and digital literacy among judges, prosecutors, and court staff. Modern solutions lead to a more accessible, transparent, and, most importantly, effective justice system. However, it is essential to remember that the digitization of law and justice presents challenges that must be considered in a digital democracy. Foremost among these are guarantees of cybersecurity and the protection of personal data, which underpin public confidence in justice. In this case, it is of utmost importance to create and provide access to systems that ensure the highest standards of cybersecurity. Digitization also requires a change in mentality and skills, on the part of the participants in proceedings and their representatives, and above all on the part of legal professionals (in particular judges and prosecutors) and administrative staff. The digital transformation of law and the judiciary is one of the most critical manifestations of e-democracy. However, it must be implemented responsibly, ensuring a balance between innovation and the protection of fundamental rights and freedoms. Its success depends on maintaining a balance between technological innovation and the protection of fundamental rights and procedural guarantees. The principles of transparency, proportionality, and accountability must remain central to all reforms to ensure that efficiency never undermines the rule of law or judicial independence.

4. Digital reforms in the Lithuanian judiciary

On 2 December 2022, the European Commission adopted the Communication on Digitalisation of Justice in the European Union (Vėbraitė & Strikaitė-Latušinskaja, 2023). Over the past two decades, Lithuania has implemented wide-ranging reforms to modernize its court administration – from electronic filing to AI-driven tools – while grappling with issues of equality, ethics, and infrastructure (Gaubienė,

2023, p. 7–9.). Lithuania began investing early in court IT systems. The Lithuanian Courts Information System (LITEKO), launched in 2004, created a unified electronic case registry for all courts (Vėbraitė, 2020). Building on this foundation, the country introduced the Electronic Services Portal for Courts (e.teismas), which enables the online filing of documents, tracking of case progress, and electronic service of judicial documents. Adoption of e-filing has skyrocketed – by 2022, 86% of all civil and administrative cases in Lithuania were handled electronically via the e.teismas portal (Greičienė, 2023). This high uptake reflects both strong institutional support and user acceptance of digital case management. Courts have also adopted virtual hearings, which were accelerated by the COVID-19 pandemic (Vėbraitė, 2020). Under Article 34(7) of the Law on the Courts of the Republic of Lithuania, the hearing of cases and the participation of the persons involved in the case can be ensured using ICT (through video conferences, teleconferences, etc.), in accordance with the procedure established by the Minister of Justice, coordinated with the Council of Judges. Using these technologies, reliable identification of the persons participating in the case, objective recording and presentation of data (evidence), and access to procedural rights and publicity of the trial in court, as well as confidential communication with the lawyer (representative) for the persons participating in the case, must be ensured. Further, Article 34(8) of this Law stipulates that when the case is examined through oral proceedings using secure ICT (via video conferences, teleconferences, etc.), the members of the panel of judges can participate in the court session from different premises of the court. During such hearings, the persons participating in the case may be in different court or non-court premises. Moreover, Article 37(1)(1) states that electronic data related to court proceedings are processed, recorded, and stored in courts using ICT, in accordance with the procedure established by the Council of Judges, coordinated with the Chief Archivist of Lithuania.

The Lithuanian Code of Civil Procedure not only explains how electronic communication technologies are used in civil procedures, but also promotes the possibility of initiating a case electronically, as Article 80(7) states a particular economic benefit: when procedural documents and their annexes to the court are submitted only by an electronic means of communication, and when a wish to receive procedural documents only by these means is expressed, only 75% of the amount of the stamp duty has to be paid. Article 175(1) explains how electronic communication technologies are used in civil procedures. Article 175(2) specifies that the examination of cases and the participation of persons participating in the case may be ensured by using ICT (via video conferences, teleconferences, and otherwise), in accordance with the procedure established by the Minister of Justice, coordinated with the Judicial Council. To sum up, videoconferencing is now widely used in court activities, enhancing transparency by enabling the public to observe remote hearings online in real time (Greičienė, 2023). This also supports the possibility of saving time and costs for the procedure.

Innovations in criminal procedure law have also gone hand in hand with those in civil procedure. Article 8(1) of the Lithuanian Code of Criminal Procedure implemented the possibility of processing criminal case data and serving procedural documents using ICT. Article 8(2) allows the use of ICT in criminal proceedings. Attention should be drawn to the position of the European Court of Human Rights, which, in its case law referring to videoconferencing as a form of participation by the accused in criminal proceedings, notes that as a general rule, this is incompatible with the concept of a fair and public hearing. However, in the Court's view, the use of this technology must serve a legitimate aim in each case, and the procedures for providing explanations and participating in the hearing must comply with the requirements of a fair trial (Kulesza, 2021, p. 207). The digitization of the justice system as a response to contemporary challenges is indeed a permanent feature of the transformation of judicial institutions. Digitization and the use of modern technological tools must not lead to a lowering of the standards that result from Article 6 of the ECHR, i.e. the right to a fair trial (European Union, 1950[)].

Most recently, Lithuania has ventured into AI applications within the judiciary – albeit in a cautious and supplementary manner. In January 2025, the Lithuanian Supreme Court launched a pilot AI system called 'TeDIA', an acronym for Teismo Dirbtinio Intelekto Įrankis (Court' AI Tool). TeDIA is essentially a virtual assistant for drafting court press releases: it uses the court's judgments and orders to automatically generate summaries for the website mediakf.vu.lt. This allows the Court's communications to be faster and more consistent. Crucially, TeDIA does not engage in deciding cases or recommending outcomes – its function is limited to disseminating post-decision information. This reflects the broader Baltic approach to judicial AI: the current uses of AI in Baltic courts are 'primarily for auxiliary, technical tasks' (Institute of Law at the Lithuanian Centre for Social Sciences, n.d.) rather than for core judicial decision-making. The development of TeDIA was a collaborative effort, involving the National Courts Administration and researchers (including a project with Vilnius University), to ensure the tool met quality and ethical standards (Lietuvos Teismai, 2024). The introduction of such an AI assistant, reportedly one of the first of its kind in EU judicial systems, exemplifies Lithuania's innovative yet cautious approach to legal technology. It shows how automation can assist judges and staff by handling routine writing tasks, while leaving judicial decisions entirely in human hands.

One of the biggest challenges has been ensuring that the technological infrastructure and security keep pace with the increasing number of new digital workloads. The National Courts Administration has pursued infrastructure improvements and capacity-building; by 2023, most courtrooms were equipped for high-quality videoconferencing, and digital audio recording of hearings became standard practice. These upgrades not only facilitate remote proceedings but also improve the record-keeping and transparency of in-person trials, by replacing handwritten minutes with verbatim audio records. Ensuring cybersecurity has been another priority: Lith-

uanian courts have implemented stronger data protection measures (secure case management servers, encrypted communications) in line with GDPR and national cyber guidelines. Notably, the judiciary has so far avoided any significant data breach, a result of proactive security planning that other countries can emulate.

The introduction of AI tools like TeDIA has also brought ethical and legal questions to the forefront. Lithuanian judicial leaders have emphasized a cautious approach: any use of AI must be thoroughly assessed for its added value and potential risks, with human rights and personal data strictly protected (Limantė et al., 2025). Before deploying TeDIA, the Supreme Court undertook extensive consultations and pilot testing to ensure the AI' summaries were accurate and unbiased. The project team established that the AI would not access any confidential information beyond final published decisions, mitigating privacy concerns. Additionally, judges retain complete oversight: they can edit or veto an AI-generated press release before it is published. By keeping a human in the loop, Lithuania has managed to benefit from automation while upholding judicial accountability. The early success of TeDIA, in terms of positive feedback and time saved for staff, suggests that, with proper safeguards, AI can be a helpful servant to justice, not a threat.

The Lithuanian Courts Administration is actively investing in enhancing judges' digital and AI literacy. In 2025, introductory training for newly appointed judges included an eight-hour programme on 'Artificial Intelligence and Personal Data Protection', covering the use of AI in judicial work (Judicial Council of Lithuania, 2024). Additional training programmes have addressed AI tools in court operations and the impact of digitalization on the legal system. Notably, the seminar 'AI and the Judiciary: Exploring Possibilities and Pitfalls' was held in Vilnius on 12–14 May 2025 as part of the Advanced Training in EU Law for Judges and Prosecutors, organized by the Academy of European Law (2025).

5. Digital reforms in the Polish judiciary

For many years, new technologies have been implemented in the judiciary, aiming in particular to streamline court proceedings, replace the traditional form of recording procedural activities by using modern technological solutions, increase the transparency of court proceedings, introduce properly documented case files enabling a correct assessment of the conducted proceedings, shorten the duration of recorded court hearings, and reduce the costs of proceedings (Karolczuk, 2018, p. 37). Over the past decade, there have been significant changes in the use of IT systems in court proceedings in Poland (Bartoszek, 2022, p. 15; Kotalczyk, 2021, p. 61) and – as mentioned above – in Lithuania.

One of the key elements of digital democracy in Poland is the Random Case Allocation System (SLPS), which has been in effect in Poland since 2018. In §2, point

16 of the Regulation of the Minister of Justice of 18 June 2019, the SLPS was defined as an IT system used for the random allocation of cases and court tasks, operating based on a random number generator.[1] This means that there is no possibility of interfering in the draw process, which takes place automatically; therefore the SLPS combines the principle of randomness with the principle of proportional allocation of cases (Gov.pl, 2021). Until the introduction of the SLPS, the president of a court or the chairman of a department decided who was to handle a given case, which raised many concerns. In the SLPS's current form, a citizen can be confident that which case goes to which person depends on the IT system.

The computerization of the Polish judiciary with the SLPS involves not only the random assignment of cases but also provides citizens with access to the reporting module. Any interested person can access the reports free of charge via the Information Portal and the Ministry of Justice's website, after selecting the appropriate court and department and entering the case reference number under which it was registered in the SLPS (Gov.pl, 2022). This solution deserves our approval. At the same time, there is a lack of instructions in this area, as access to the data is not possible without entering the case reference number. Citizens typically do not know the rules for assigning reference numbers, and the search engine itself does not provide any instructions and lacks intuitive functionality. In this respect, it would be necessary to add a legend and explain the individual solutions for people who do not have specialist knowledge in this area.

Another example of the computerization of the Polish judiciary is the system of Electronic Writ of Payment (Elektroniczne Postępowanie Upominawcze), Electronic Land and Mortgage Registers (Elektroniczne Księgi Wieczyste), and the electronic National Court Register (Elektroniczny Krajowy Rejestr Sądowy). Procedural documents are also made available to professional attorneys on the Information Portal. Additionally, it is possible to hold hearings remotely, as discussed in more detail in section 3 of this article. An e-protocol has also been introduced in Polish courtrooms, consisting of recording the course of a hearing; however, there are no solutions for its automatic transcription. Such a solution could shorten the duration of hearings, because there is a high chance that judges would refrain from recording testimony. In addition, each person familiarizing themselves with the course of a hearing would have the option to choose a recording or a written protocol (Kotalczyk, 2021, p. 61). The popularization of recording hearings and e-minutes would also significantly con-

1 A short description of the algorithm, which explains the basic principles of the system, is available in the justification of the Rules of Procedure of the Common Courts. To ensure transparency, the Ministry of Justice has decided to also provide a full description of the algorithm, which is part of the project documentation. It can be found on the website of the Ministry at https://www.gov.pl/web/sprawiedliwosc/algorytm.

tribute to reducing the number of requests for corrections submitted by parties to the proceedings.

One of the IT systems used in Polish courts is the PESEL-SAD system, mainly used to determine addresses. As rightly noted in the 'Recommendations for the use of artificial intelligence in the judiciary and prosecutor's office' (Working Group on Artificial Intelligence, Subgroup on Ethics and Law, 2023, p. 17), PESEL-SAD unfortunately only has information about the current and previous registrations of a given person.

> It is reasonable to recommend integrating the PESEL-SAD system with public administration systems. It would be crucial to identify the addresses that an individual has provided when using the services of other public authorities, in particular tax authorities, the Social Insurance Institution, the National Health Fund, or municipal and regional offices, for example when applying for an identity card or passport.It would also be important to obtain information from other court proceedings regarding the address at which correspondence had previously been successfully served.Moreover, courts have access to the NOE-SAD system, which records all persons deprived of their liberty.The PESEL-SAD system should import data from it on whether the wanted person is currently imprisoned in a penitentiary unit, and if so, what address they have provided for release. Another useful functionality would be to automatically inform the court that the data of a person who is a party to the case have changed, in particular if they have changed their name or address, have been deprived of liberty, or died. (Working Group on Artificial Intelligence, Subgroup on Ethics and Law, 2023, p. 17)

In 2021, the Polish prosecutor's office implemented a system called PROK-SYS; one of its basic functions is the digitalization of files from preparatory proceedings in criminal cases. This allows the parties to view files online via the File Review Portal, which is more convenient than visiting the prosecutor's office and may increase the degree of protection of the parties' interests. The system was implemented as a supplement, not as a replacement for the paper-based file flow.

Artificial intelligence is a topic that is changing the reality around it, including the justice system in Poland. The Ministry of Justice has developed a Digital Court programme, consisting of multiple modules, with work spread over a timeline that allows for digitization to occur in stages. According to the Ministry of Justice's website, this programme aims to ensure an efficient judiciary by facilitating citizens' access to courts through the digitization of files and the automation of data verification. The idea is for the Polish judiciary to work primarily with digital documents, as storing paper court files incurs significant costs. Additionally, the goal is to provide public access to justice services via computer or telephone. At the same time, as part of the solutions being developed, mechanisms will be introduced to protect against digital exclusion, i.e. a situation in which a person cannot submit or receive documents in paper form. All changes related to the implementation of the so-called digital

court are to be first tested through a pilot, and after eliminating any potential problems, implemented nationwide. Currently, the Court of Appeal in Katowice has been tasked with developing a uniform solution for scanning and archiving files. In addition, on 3–5 April 2025, representatives of the Ministry of Justice met at the Prison Service Training Centre in Popowo to discuss the assumptions of the Digital Court programme. The training was attended by judges and officials from the district, regional, and appellate courts in Gdańsk and Warsaw.

The key phase of digitalizing Polish courts is expected to be completed within the next four years, i.e. by 2029. The modules that comprise the Digital Court programme will be discussed below. Pilot projects of the programme are already being introduced; an example is the pilot project Digital Assistant to the Judge, which is already being implemented and will be used in Swiss franc cases in courts of first and second instance. The Digital Assistant to the Judge is designed to facilitate citizens' access to court cases online, enable the electronic filing of documents, and simplify and automate office processes in court secretariats. This point provides for, among other things, the enabling of robotic writing of procedural documents to relieve court secretariats, which would be automatically entered into court systems; a knowledge base containing the cited case law of the Court of Justice of the European Union; or an algorithm enabling the creation of draft court decisions. The Ministry of Justice expects this project to be completed by mid-2026 (Portal Samorządowy, 2025).

According to Grzegorz Polak, the director of the Department of Computerization and Court Registers of the Ministry of Justice, a pilot programme for the complete digitalization of the work of the Court of Competition and Consumer Protection (SOKiK) is to be launched in 2025 (Rojek-Socha, 2025). This aims to introduce the possibility of conducting an entire case electronically. Ultimately, a central repository and office system for all ordinary courts will be created by developing a file browser that allows access to documents and enables marking, tagging, attaching notes, and filtering.

The Ministry of Justice is also working on the new Electronic Writ of payment proceedings (EPU) 3.0. The current Electronic Writ of payment proceedings allows for the entry of incorrect data. The new EPU will eliminate this possibility through integration with external registers and the use of dictionaries. In addition, activities in the area of the digitization of correspondence sent in paper form are to be improved, including the recognition of document categories and downloading data from scanned documents. Another issue being addressed is the introduction of a proxy calendar, reminder functions, and notifications (also via dedicated system interfaces) for entities handling numerous cases in the system. The Ministry of Justice website states that such solutions will be placed in the EPU by mid-2026. The Ministry of Justice also plans to transfer case files from the prosecutor's office to the court electronically, thereby expediting proceedings. The pilot phase of this project is scheduled to begin in 2025.

Transferring data to the electronic (and intangible) plane is a natural and desirable result of ongoing technological development. As a significant driver of socio-economic change, information and communication technologies are increasingly influencing the activities of public administration and justice authorities, becoming an impetus for introducing various changes in their structure and functioning (Jastrzębska, 2018, p. 36; Sieber, 2001, p. 14). This is reflected in the Act of 17 February 2005 on the computerization of the activities of entities performing public tasks (Sejm of Poland, 2005) amending this Act and certain other acts, which introduces the Committee for Digitization to systematize activities. The aim of this Act is to introduce solutions that support the digital transformation of the state, ensuring the coordination of digital development in public administration and the harmonization and complementarity of activities aimed at this end.

At the level of proceedings pending before Polish courts, it is worth paying attention to solutions that reflect the changing reality and the ongoing technological revolution. Examples of computerization in the justice system include remote hearings, regulated in Article 148[1] of the Code of Civil Procedure and Article 151 §2 of the Code of Civil Procedure. In criminal proceedings, participation in a hearing using technical devices that enable remote participation with simultaneous direct transmission of images and sound is regulated in Article 374(3) of the Code of Criminal Procedure.[2] According to this provision, the court (through the presiding judge), upon the prosecutor's request, consents to a prosecutor' participating in the hearing using technical devices enabling remote participation, provided that no technical reasons prevent this. Moreover, in accordance with Article 177 of the Code of Criminal Procedure, the examination of a witness may be carried out remotely. Another example of computerization in Poland is e-delivery. The Act of 18 November 2020 on Electronic Delivery introduces the obligation to use the National Electronic Delivery System; in Poland, this obligation will apply to courts from 1 October 2029 (Gov.pl, n.d.).

6. The role of international standards and cooperation in ensuring digital justice

2 The Act of 19 June 2020, on interest subsidies for bank loans granted to entrepreneurs affected by the effects of COVID-19 and on simplified proceedings for the approval of an arrangement in connection with the occurrence of COVID-19 (Journal of Laws of 2022, item 2141), added §§3–9 to Article 374. These provisions specify the conditions for conducting a remote hearing. It should also be noted that the possibility of conducting hearings remotely was extended to other procedural stages, including those referred to in Articles 96a and 250 §§3b–3h. It should be emphasized that although remote hearings were introduced by the aforementioned act related to the COVID-19 pandemic, the provisions in question do not include a requirement for the occurrence of difficulties or threats related to an epidemic situation. This means that a remote hearing, after meeting certain conditions, can be held in any case and has been introduced permanently, not ad hoc, into the Code of Criminal Procedure.

At the EU level (Balcerzak, 2024), Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 Laying Down Harmonized Rules on Artificial Intelligence (the AI Act) plays a huge role. According to the Regulation, AI is a rapidly developing group of technologies that contributes to numerous benefits. The justice system (Fik & Staszczyk, 2022) was also cited as an example of the benefits of using AI, with the argument that its use enables better forecasting, optimization of operations and resource allocation, and personalization of digital solutions available to individuals and organizations (Dolniak et al., 2024).

The AI Act is the world's first comprehensive legal regulation for artificial intelligence systems and models; it aims to ensure security, transparency, and compliance with European values in the development and use of AI (Gov.pl, 2024). In the area of justice, it was considered that:

> certain AI systems intended for the administration of justice and democratic processes should be classified as high-risk systems, taking into account their potentially significant impact on democracy, the rule of law, personal freedoms, as well as the right to an effective remedy and access to an impartial court. In particular, to eliminate the potential risk of bias, errors, and the black box effect, AI systems intended for use by or on behalf of judicial authorities to assist them in searching for and interpreting facts and law and in applying the law to a specific factual situation should be classified as high-risk systems. AI systems intended for use by Alternative Dispute Resolution (ADR) bodies for these purposes should also be considered high-risk if the results of the ADR procedure produce legal effects for the parties. The use of AI tools can support the decision-making powers of judges or the independence of the judiciary, but should not replace them; the final decision-making must remain a human-driven activity. However, the qualification of AI systems as high-risk AI systems should not extend to AI systems intended for purely auxiliary administrative activities that have no impact on the actual administration of justice in individual cases, such as anonymisation or pseudonymisation of court decisions, documents or data, communications between staff members, administrative tasks. (AI Act, paragraph 61)

Regarding the computerization of the justice system, the perspective of Article 6 ECHR is crucial, particularly the first paragraph, which outlines the general requirements for the fairness of court proceedings (Clifford Chance and Helsinki Foundation for Human Rights, 2021). Bearing the above in mind, it should be indicated that the following are required: an impartial and independent court; a court established by law; the right of access to a court and the right to fair court proceedings; the right to have a case heard without undue delay; and the right to a public hearing. We also must not forget Article 47 of the Charter of Fundamental Rights: Everyone whose rights and freedoms guaranteed by the law of the Union are violated has the right to an effective remedy before a tribunal. In addition, everyone is entitled to a fair and public hearing within a rea-

sonable time by an independent and impartial tribunal previously established by law. There' is no doubt that the level of digitalization across all social functions has increased dramatically in recent years. One of the driving forces behind this was the COVID-19 pandemic, which saw the increasingly digital nature of public and private services. On 30 April 2024, Regulation (EU) 2024/1183 (eIDAS 2.0) was published in the Official Journal of the European Union, entering into force on 20 May 2024. This aims to ensure that digital identities are secure and protected against fraud and unauthorized access. One of the possible areas of application is identity confirmation on public portals to quickly and safely use the services available there and to access public registers in any European Union country. Poland is integrating new regulations with the mObywatel system, and their full implementation requires an amendment to national law, initially planned for the second quarter of 2026.

These issues can be presented using examples from Polish solutions. One of the key elements of the computerization of the Polish judiciary is the SLPS. The legal basis for the solutions introduced was the regulation of the Minister of Justice amending the regulation on Rules of Procedure of Common Courts of 28 December 2017, which implemented the Council Framework Decision 2001/470/EC of 28 May 2001 establishing a European Judicial Network in civil and commercial matters within the scope of its regulation. This provision was amended by Decision no. 568/2009/EU of the European Parliament and of the Council of 18 June 2009, which states that the reason for establishing a European Judicial Network in civil and commercial matters is the creation of an area of freedom, security, and justice, and which, in order to facilitate access to justice and judicial cooperation in civil matters, calls for further efforts through the Hague Programme, adopted by the European Council at its meeting on 4 and 5 November 2004 (Pytlewska, 2019, p. 268), among others. The Hague Programme aims to strengthen the collective capacity of the European Union and its Member States to guarantee fundamental rights, minimum procedural safeguards, and access to justice. Point 3 of the Programme, under the heading of strengthening justice, identifies the need to intensify further work on creating a Europe for citizens and the key role that the establishment of a European area of justice plays in this respect (European Union, 2005). The document that indicated the automatic allocation of cases as a guarantee of impartiality was Recommendation no. CM/Rec(2010)12 of the Committee of Ministers (Council of Europe, n.d.). According to point 24 of this recommendation, the allocation of cases within a given court should be based on objective, previously established criteria, to ensure the right to an independent and impartial court; it should not yield to the wishes of the parties or anyone else interested in the course of the proceedings. The use of an electronic case management system and communication technologies, which the authorities and judges should promote, was recommended as a way to facilitate such allocation (point 37).

To introduce modern solutions in the field of digitalization of the judiciary, in 2023 the Minister of Justice established an interdisciplinary team for the imple-

mentation of modern technologies; the legal basis for its operation is the Minister of Justice's order of 17 October 2024.[3] The tasks of this team include, in particular, an analysis of needs in the field of the use of modern technologies in the justice system and the development of recommendations in this area, as well as defining and analysing the main barriers (legal, technological, organizational, or personnel) hindering the implementation of modern technologies in the justice system.

On 16 October 2024, a draft act on artificial intelligence systems was introduced in Poland, and is currently undergoing public consultation. On 28 April 2025, an agreement was signed between the Ministry of Justice and the Ministry of Digital Affairs under which the digital transformation of the justice system wilented. Additionally, the Ministry of Digital Affairs has prepared a draft of a new Artificial Intelligence Development policy for Poland, covering the period up to 2030. As we can read there, a wise and responsible implementation of AI in the Polish justice system can enhance the work of judges and prosecutors, reduce the duration of proceedings, and facilitate 'easier and faster access to these institutions by citizens. The draft AI policy was available for public consultation until 1 July 2025. In this context, it is also worth noting the 'State Digitalization Strategy to 2035', which states that the development of artificial intelligence is one of the key areas in Poland's digital transformation. The implementation of the latest technologies and the use of systems based on human-centric, sustainable, trustworthy, and safe artificial intelligence are crucial for the country's development. For this to become possible, it is necessary to determine the direction of state policy and ensure its proper coordination and implementation. In Poland, the key phase of digitalizing the courts is expected to be completed within the next four years, i.e. by 2029. Intensive work is currently underway in this area, so the coming years will bring verification of the extent to which the declared functionalities will be implemented and, above all, to what extent the changes will be beneficial to society.

Conclusions

The future of digital democracy – whether it ends in success or failure – depends on whether digital spaces for civic participation are designed appropriately. They must take into account the complexity of democratic processes so that technology supports and strengthens democratic institutions rather than undermining them (Squeo, 2023, p. 92). This means that technology itself does not determine the quality of democracy; it is how it is used and integrated into existing structures that influences the outcome. Digital tools (such as consultation platforms, online voting systems, and dedicated ICT systems) have the potential to support democracy by increasing access to information,

3 The legal basis for its operation is the order of the Minister of Justice of 16 October 2023, item 196., the order of the Minister of Justice of 17 October 2024, item252), and the order of the Minister of Justice of 19 February 2025, item 10).

promoting transparency, and developing citizen participation. However, if poorly designed, they can also foster disinformation and polarization, and undermine trust in institutions. For this reason, a systemic approach and conscious design of digital spaces, taking into account their social, political, and legal impacts, are crucial. It is not just about technology, but about understanding its interaction with human behaviour, political culture, and governance mechanisms.

The first hypothesis, that digital transformation of the judiciary can enhance the rule of law provided that transparency is maintained, has been confirmed. The computerization of court proceedings is a multi-level process. It not only contributes to streamlining court proceedings and work, but also increases the transparency of case handling. Moreover, and extremely important from the citizen's point of view, it can have a positive impact on the duration of court proceedings. Unfortunately, like any new technology, it also brings risks. The biggest challenge for computerizing court proceedings is the building of safeguards that protect parties from the leaking of their personal data and case information to unauthorized persons, while also integrating existing systems to ensure the entire system operates even faster and more transparently (Karolczuk, 2018, p. 37).

Therefore a diagnosis of the needs of the justice system is crucial. The last hypothesis has been confirmed; according to the 'Survey of expectations regarding automation of work in IT systems in courts' report (Ministerstwo Sprawiedliwości, n.d.), which was conducted by the IT and Court Records Division of the Court Service Development Department of the Ministry of Justice in the form of a questionnaire (with 1,848 responses) published on the website between 10 May and 30 June 2023, the needs of the judiciary are diverse. In particular, significant differences can be observed in the use of the IT systems in question depending on the organizational unit. As Reiling believes, 'delay, access, and corruption are three crucial issues any judicial organization or court faces. They are the three most common complaints of court users around the world' (2009). The future of the judiciary is increasingly shaped by digital transformation. Court records will be kept in electronic form, and cases will be held through video conferences. Other electronic instruments to accelerate the course of the proceedings will also start to be used (Wrzaszcz, 2023).

In Poland, the next phase of reform will determine not only whether the planned digital infrastructure is successfully implemented, but also whether it genuinely enhances access to justice and procedural efficiency.. The most anticipated changes, considered the most important (in principle), involve the automation of activities that allow for the determination of the most essential information about the participants in proceedings as broadly understood, most often by obtaining information from external databases (PESEL, Civil Registry, Central Register and Information on Economic Activity (CeiDG), etc.), as well as court records and office systems (with knowledge about the participants' involvement in other proceedings). Another widely anticipated set of functionalities is those designed to facilitate the conversion

of paper documents into an editable digital form. Compared to Poland, Lithuania is further advanced in digitizing its justice system; it represents a more coherent approach to digital justice, oriented to the rule of law, whereas Poland's reforms remain fragmented and politically influenced. While Poland plans to complete the key stage of the digital transformation of courts by 2029, Lithuania has already implemented several solutions that are still in the planning or pilot phase in Poland. The Lithuanian e-court system (e.teismas) enables, among other things, complete online case management, the electronic filing of pleadings, and remote access to case files by the parties. The Lithuanians have successfully integrated court systems with public registers (such as the PESEL register or the business register), which allows for the automatic retrieval of data on participants in proceedings without requiring court staff to identify them each time. It is this aspect – the automation of obtaining data on proceeding participants – that is also recognized in Poland as one of the most important goals of computerization. Lithuania has also made significant progress in document processing, implementing systems that enable the automatic recognition and digitization of paper documents, which supports document circulation and archiving in office management systems. It is worth noting that Lithuania attaches great importance to cybersecurity and personal data protection, which aligns with concerns expressed in the Polish context, especially regarding the risk of unauthorized access to the data of parties to proceedings. Thanks to centralized IT infrastructure management and standardization of solutions, Lithuanians have created a more coherent and secure digital justice ecosystem.

The analysis confirms that the digitization of the justice system is an ambiguous phenomenon: on the one hand, it has real potential to improve the functioning of courts and increase their accessibility and transparency, and on the other hand, it may lead to the erosion of fundamental procedural guarantees if implemented without adequate institutional and legal safeguards. Verification of this hypothesis has shown that digital technologies, such as the automation of court proceedings, remote access tools, and decision-support systems, can strengthen the rule of law, provided that they are introduced transparently and proportionately, with the constitutional and conventional standards of a fair trial. In both Poland and Lithuania, it is crucial to ensure that the digitization process is not an end in itself, but a means to achieve the fundamental values of a democratic state governed by the rule of law. In this context, it is essential not only to design technology, but also to maintain mechanisms for citizen control, judicial oversight, and open dialogue, including with the legal community and the general public. The case of Lithuania, a country with a more advanced level of judicial digitization, demonstrates that properly designed reforms can increase efficiency without compromising the rights of parties, thereby serving as an inspiration for other Member States. In the long term, it will be crucial not only to monitor the impact of the technological solutions implemented but also to systematically assess their compliance with the rule of law, which requires cooper-

ation between legislatures, the judicial administration, practitioners, and international institutions. The literature indicates that at present, another critical challenge lies ahead: the judiciary should be supported with electronic instruments that would allow cases to be analysed by a system that proposes a procedural decision to end the case (Wrzaszcz, 2023).

Considering the above considerations, it seems worthwhile creating a list of recommendations, in particular:

1) Introducing a unified legal framework for digital tools in the judiciary.
2) Establishing rules for the use and transparency of AI in judicial processes.
3) Providing digital literacy and ethics training for judges and court staff.
4) Strengthening citizen oversight and participatory mechanisms in digital reforms.
5) Aligning national regulations with European standards (ECHR, EU AI Act, Charter of Fundamental Rights).

REFERENCES

Academy of European Law (ERA) (2025). *Advanced Training in EU Law for Judges and Prosecutors: Preliminary Ruling Procedure, Charter of Fundamental Rights and the Rule of Law* (Vilnius, 12–14 May 2025)

Balcerzak, M., & Kapelańska-Pręgowska, J. (2024). *Artificial intelligence and international human rights law: Developing standards for a changing world*. Edward Elgar. https://www.elgaronline.com/edcollbook-oa/book/9781035337934/9781035337934.xml

Bartoszek, M. (2022). Application of artificial intelligence in the judiciary in the light of the principle of effective judicial protection. *Folia Iuridica Universitatis Wratislaviensis*, *11*(1), p. 8–29. https://bibliotekacyfrowa.pl/Content/133810/PDF/Folia_Iuridica_Universitatis_Wratislaviensis_2022_vol_11_no_1.pdf?

Chałubińska-Jentkiewicz, K. (2019) Komentarz do art. 48 CyberbezpU. In W. Kitler, J. Taczkowska-Olszewska, & F. Radoniewicz (Eds.), *Ustawa o krajowym systemie cyberbezpieczeństwa. Komentarz* (pp. 292–302). Warsaw.

Clifford Chance and Helsinki Foundation for Human Rights (2021). *New technologies. New justice. New questions. Implementation of new technologies in the justice system*. Clifford Chance and Helsinki Foundation for Human Rights. https://hfhr.pl/upload/2021/09/raportnn_en1ocoscreen_1.pdf?

Constitution of the Republic of Poland (Journal of Laws of 1997, no. 78, item 483).

Council of the European Union (2001). Council Decision 2001/470/EC of 28 May 2001 establishing a European Judicial Network in civil and commercial matters, OJ L 174, 27.6.2001, p. 25–31.

Council of Europe. (n.d.) *TITLE*. https://search.coe.int/cm#{%22CoEIdentifier%22:[%2209000016805b1524%22], %22sort%22:[%22CoEValidationDate%20Descending%22Dolniak, P., Kuźma T., Ludwiński, A., & Wasik, K. (2024). *Sztuczna inteligencja w wymiarze sprawiedliwości. Między prawem a algorytmami*. Wolters Kluwer Polska.

Eltis, K. (2023). Judicial independence and the corporate 'custodians' of digital tools: A call to scrutinize reliance on private platforms as 'essential infrastructure'. In C. Castets-Renard & J. Eynard (Eds.), *Artificial intelligence law between sectoral rules and comprehensive regime: Comparative law* (pp. 1–12). Bruylant. https://ssrn.com/abstract=4599274

European Commission. (2025, 16 January). *European e-justice strategy 2024–2028* (O. J. C 2025/437). https://data.europa.eu/eli/C/2025/437/oj

European Commission for the Efficiency of Justice (CEPEJ). (2018). *European ethical charter on the use of artificial intelligence in judicial systems and their environment*. https://www.europarl.europa.eu/cmsdata/196205/COUNCIL%20OF%20EUROPE%20-%20European%20Ethical%20Charter%20on%20the%20use%20of%20AI%20in%20judicial%20systems.pdf

European Commission for the Efficiency of Justice (CEPEJ). (2021). *Guidelines on electronic court filing (e-filing) and digitalisation of courts* (CEPEJ(2021)15). https://rm.coe.int/e-filing-en/1680b2calcEuropean Network of Councils for the Judiciary (ENCJ). (2017, 31 March). *Justice seminar in the District Court of Amsterdam*. https://www.encj.eu/articles/87

European Parliament. (2016). Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (GDPR).

European Parliament. (2022). Decision (EU) 2022/2481 of the European Parliament and of the Council of 14 December 2022 Establishing the Digital Decade Policy Programme 2030 (O. J. L 323, 19.12.2022, pp. 4–26).

European Parliament (2022), Decision (EU) 2022/2081 of the European Parliament and of the Council of 14 December 2022 establishing the 2030 Policy Programme 'Path to the Digital Decade', OJ L 323, 19.12.2022, pp. 4–26.European Parliament. (2024). Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 Laying Down Harmonised Rules on Artificial Intelligence and Amending Certain Legislative Acts (Artificial Intelligence Act) (O. J. L 1689/1).

European Union. (1950). *European convention for the protection of human rights and fundamental freedoms* (O. J. C 2010/83, p. 389).

European Union. (2000). Charter of Fundamental Rights of the European Union, proclaimed on 7 December 2000, OJ C 364, 18.12.2000, pp. 1–22.

European Union. (2005.) The Hague Programme: Strengthening freedom, security and justice in the European Union, European Council, 4–5 November 2004, OJ C 53, 3.3.2005, pp. 1–14.

European Union. (2014.) Regulation (EU) no. 910/2014 of the European Parliament and of the Council of 23 July 2014 on Electronic Identification and Trust Services for Electronic Transactions in the Internal Market and Repealing Directive 1999/93/EC (OJ 2014 L 257).

Fik, P., & Staszczyk, P. (2022). Sztuczna inteligencja w unijnej koncepcji e-sprawiedliwości – teoria i możliwy wpływ na praktykę. *Europejski Przegląd Sądowy*, *7*, 4–9.

Friedland, L. A. (1996). Electronic democracy and the new citizenship. *Media, Culture & Society*, *18*(2), 185–212. https://doi.org/10.1177/016344396018002002

Gaubienė, N. (2023). Digital transformation of enforcement procedures of court decisions and search for efficiency. *Przegląd Prawa Egzekucyjnego*, *7*, 7–36.

Gov.pl. (2021, 16 September). *System Losowego Przydziału Spraw wyeliminował patologie w sądownictwie*. https://www.gov.pl/web/sprawiedliwosc/system-losowego-przydzialu-spraw-wyeliminowal-patologie-w-sadownictwie

Gov.pl. (n.d.). *E-doręczenia: Harmonogram*. https://www.gov.pl/web/e-doreczenia/harmonogram

Gov.pl. (2022, 22 October). *Wyszukiwarka raportów z Systemu Losowego Przydziału Spraw*. https://www.gov.pl/web/sprawiedliwosc/wyszukiwarka-raportow-z-systemu-losowego-przydzialu-spraw

Gov.pl. (2024, 1 August). *Rewolucja w regulacji: wchodzi w życie Akt o AI*. https://www.gov.pl/web/ai/rewolucja-w-regulacji-wchodzi-w-zycie-akt-o-ai

Greičienė, J. (2023, 20 October). *Development of digital technologies increases the accessibility of the justice system*. Ministry of Justice of the Republic of Lithuania. https://tm.lrv.lt/en/news/jurga-greiciene-development-of-digital-technologies-increases-the-accessibility-of-the-justice-system

Hagen, M. (1997). *A typology of electronic democracy*. http://martin-hagen.net/publikationen/elektronische-demokratie/typology-of-electronic-democracy/

Horváth, M., Hlásny, M., & Krásna, S. (2025). Strengthening the rule of law for the future of democracy: Anticipated trends in law in the digital era. *Acta Educationis Generalis*, *15*, pp. 106–120. https://doi.org/10.2478/atd-2025–0017

Institute of Law at the Lithuanian Centre for Social Sciences. (n.d.). *News: A new article by Institute researchers examines AI applications and development trends in the judicial systems of the Baltic States*. https://teise.org/en/20250423–2

Janssen, M., & van den Hoven, J. (2015). Big and Open Linked Data (BOLD) in government: A challenge to transparency and privacy? *Government Information Quarterly*, *32*(4), 363–368. https://doi.org/10.1016/j.giq.2015.11.007

Jastrzębska, K. (2018). *Elektroniczna administracja jako narzędzie wdrażania zmian organizacyjnych*. Wydawnictwo Uniwersytetu Łódzkiego. .

Judicial Council of Lithuania. (2024, 27 September Teisėjų taryba (2024 m. rugsėjo 27 d.). Nutarimas Nr. 13P-134-(7.1.2) „Dėl 2025 metų teisėjų mokymo programų patvirtinimo ir Teisėjų tarybos 2024 m. sausio 26 d. nutarimo Nr. 13P-12-(7.1.2) „Dėl įvadinių teisėjų mokymo programų patvirtinimo“ pripažinimo netekusiu galios“. Vilnius. https://www.teismai.lt/data/public/uploads/2024/10/tt-nutarimas-ir-mokymu-programos.pdf

Karolczuk, J. (2018). Informatyzacja postępowania sądowego. Szanse i zagrożenia, *Młody Jurysta – numer specjalny – I Konferencja Młodych Naukowców Prawa Administracyjnego*, *4*, 37.

Kotalczyk, M. (2021). Artificial intelligence in the service of the Polish court: Proposed solutions. *Iustitia*, *2*, 61.

Kulesza, C. (2021). Rozprawa zdalna oraz zdalne posiedzenie aresztowe w świetle konwencyjnego standardu praw oskarżonego. *Białostockie Studia Prawnicze*, *26*(3), pp. 75–92.

Lietuvos Teismai. (2024, 18 November). *Naujienos: Lietuvos Aukščiausiajame Teisme pristatytas Teismo dirbtinio intelekto įrankis ‘TeDIA’*. https://www.lat.lt/naujienos/lietuvos-auksciausiajame-teisme-pristatytas-teismo-dirbtinio-intelekto-irankis-tedia/1869

Limantė, A., Šukytė, M., & Gaubienė, N. (2025). *Dirbtinis intelektas teismuose: teorija, praktika ir teisinis reguliavimas, Vilnius*. https://teise.org/wp-content/uploads/2025/06/DI_teismuose.pdf

Małecka-Łyszczek, M. (2024). Aksjologiczne umocowanie inkluzji cyfrowej. In A. Gryszczyńska, G. Szpor, & W. Wiewiórowski (Eds.), *Internet. Solidarność cyfrowa. Digital solidarity* (pp. 45–60). C.H. Beck Polska.

Minister of Justice in Poland (2017), Regulation of the Minister of Justice of 28 December 2017 – Rules of Procedure of Common Courts (Journal of Laws 2017, item 2487).

Minister of Justice in Poland. (2019). Ordinance of 18.06.2019: Regulations of the Official Procedure of Common Courts (Journal of Laws of 2024, no. 867).

Minister of Justice in Poland. (2023). The order of the Minister of Justice of 16 October 2023 on the Establishment of an Interdisciplinary Team for the Implementation of Modern Technologies (Official Journal of the Minister of Justice 2023, item 196).

Minister of Justice in Poland. (2024). The order of the Minister of Justice of 17 October 2024 Amending the Order on the Establishment of an Interdisciplinary Team for the Implementation of Modern Technologies (Official Journal of the Minister of Justice 2024, item 252),

Minister of Justice in Poland. (2025). The order of the Minister of Justice of 19 February 2025 Amending the Order on the Establishment of an Interdisciplinary Team for the Implementation of Modern Technologies (Official Journal of the Minister of Justice 2025, item 10).

Ministerstwo Sprawiedliwości. (n.d.). *Automatyzacja i cyfryzacja postępowań sądowych wyniki badania w sądach*. Pp. 1–102. https://www.si-dla-sprawiedliwosci.gov.pl/publikacja-ms-raport-z-badania-oczekiwan-w-zakresie-automatyzacji/

Mukhtar, M., & Siddiqah, A. (2024, 22 October). *Critically evaluate the use of AI in judicial proceedings*. http://dx.doi.org/10.2139/ssrn.4995240

Mummalaneni, V., & Challa C. (2024). ICT and access to justice: The role of telelaw in empowering vulnerable populations. *Global Journal of Business Disciplines*, *8*(1), pp. 78–90.

Musiał-Karg, M., & Kapsa, I. (2020). Attitudes of Polish voters towards introduction of e-voting in the context of political factors. In S. D. J. Barbosa, J. Filipe, A. Ghosh, I. Kotenko, & L. Zhoum (Eds.), *E-democracy – Safeguarding democracy and human rights in the digital age: 8th international conference, e-democracy 2019 Athens, Greece, December 12–13, 2019 proceedings* (pp. 137–148). Springer Nature Switzerland. https://doi.org/ 10.1007/978–3-030–37545-4_11

Pianini, D., & Omicini, A. (2019). Democratic process and digital platforms: An engineering perspective. In P. Contucci, A. Omicini, D. Pianini, & A. Sîrbu (Eds.), *The future of digital democracy: An interdisciplinary approach* (pp. 69–84). https://doi.org/10.1007/978–3-030–05333-8

Porębski, L. (2013). Rozwój elektronicznej administracji jako element zróżnicowania regionalnego. *Studia Regionalne i Lokalne*, *3*, 5–23.

Portal Samorządowy. (2025, 19 March). *Ministerstwo Sprawiedliwości przedstawiło plany dot. cyfryzacji sądownictwa*. https://www.portalsamorzadowy.pl/polityka-i-spoleczenstwo/ministerstwo-sprawiedliwosci-przedstawilo-plany-dot-cyfryzacji-sadownictwa,603091.html

Pytlewska, M. (2019). The random case allocation system as a guarantee of the impartial right to a court in the context of the European Union recommendations. *Prawo w Działaniu Sprawy Cywilne*, *40*, 268.

Reiling, D. (2009). *Technology for justice: How information technology can support judicial reform*. Leiden University Press and Amsterdam University Press.

Rejmaniak, R. (2021). Bias in artificial intelligence systems. *Białostockie Studia Prawnicze*, *26*(3), 183–198. https://doi.org/10.15290/bsp.2021.26.03.12

Rojek-Socha, P. (2025, 4 April). *Polak: Jeszcze w 2025 roku cyfrowy Sąd Ochrony Konkurencji i Konsumentów*. Prawo.pl. https://www.prawo.pl/prawnicy-sady/cyfryzacja-sadow-apelacja-przez-portal-informacyjny-wywiad-z-grzegorzem-polakiem,532330.html

Ronchi, A. M. (2019). *E-democracy: Toward a new model of (inter)active society*. Springer Nature Switzerland. https://doi.org/10.1007/978–3-030–01596-1

Sejm of Poland (2005). Act of 17 February 2005 on the Computerization of the Activities of Entities Performing Public Tasks (Journal of Laws of 2005, no. 64, item 565). Sieber, U. (2001). The emergence of information law. In E. Lederman & E. Shampira (Eds.), *Law, information and information technology* (pp. 1–36Kluwer Law International.

Skoczylas, D. (2023). *Krajowy system cyberbezpieczeństwa*. C.H. Beck Polska.

Socol de la Osa, D. U., & Remolina, N. (2024). Artificial intelligence at the bench: Legal and ethical challenges of informing – or misinforming – judicial decision-making through generative A. I. *Data & Policy*, *6*, e59. https://doi.org/10.1017/dap.2024.53

Squeo, G. (2023). *The design of digital democracy*. Springer Textbooks in Law. https://doi.org/10.1007/978–3-031–36946-9

Susskind, R. E. (2019). *Online courts and the future of justice*. Oxford University Press.

Szostek, D. (2021a). Is the traditional method of regulation (the legislative act) sufficient to regulate artificial intelligence, or should it also be regulated by an algorithmic code? *Białostockie Studia Prawnicze*, *36*(3), 45.

Szostek, D. (Ed.). (2021b). *Legal tech. Czyli jak bewzpiecznie korzystać z narzędzi informatycznych w organizacji, w tym w kancelarii oraz dziale prawnym*. C.H. Beck Polska pp. 1–480

Vėbraitė, V. (2020). Impact of the COVID-19 pandemic on court proceedings in Lithuania. *Access to Justice in Eastern Europe*, *2–3*, 156–159. https://doi:10.33327/AJEE-18–3.2–3-n000032

Vėbraitė, V., & Strikaitė-Latušinskaja, G. (2023). Digitalization of justice in Lithuania. In Vėbraitė, V., & Strikaitė-Latušinskaja, G. *Impact of the COVID-19 pandemic on justice systems: Reconstruction or erosion of justice systems* (pp. 223–234). V&R unipress. https://doi.org/10.14220/9783737015820.223

Viegas, R. B., Abrucio, F. L., Loureiro, M. R. G., Teixeira, M. A. C., & Borali, N. (2022). The communication of courts of accounts and prosecution services on social media: The challenges of accountability in the digital democracy. *Brazilian Journal of Public Administration*, *56*, pp. 342–348http://dx.doi.org/10.1590/0034–761220210320x

Working Group on Artificial Intelligence, Subgroup on Ethics and Law. (2023). *Report:* Rekomendacje dotyczące wykorzystania sztucznej inteligencji w sądownictwie i prokuraturze (eng. *Recommendations on the use of artificial intelligence in the judiciary and prosecutor's office)*. Ministry of Justice of the Republic of Poland..

Wrzaszcz, P. (2023). E-justice in Poland: Polish experiences. *Teka Komisji Prawniczej PAN Oddział w Lublinie*, *16*(1). Pp. 381–398 https://ojs.academicon.pl/tkppan/article/view/5288