UDC 342.7:004.9(4)(477)
DOI: https://doi.org/10.31359/1993-0909-2025-32-4-84

Oleg V. Sinegubov
National Academy of Legal Sciences of Ukraine
Kharkiv, Ukraine

Kharkiv Regional Military Administration
Kharkiv, Ukraine

Oksana G. Bortnik
Department of Civil, Labour and Commercial Law
Kharkiv National University of Internal Affairs
Kharkiv, Ukraine

Olena M. Chernenko
Department of Public Management, Administration and Law
National University «Yuri Kondratyuk Poltava Polytechnic»
Poltava, Ukraine

Department of Law
Private Higher Educational Institution «European University»
Kyiv, Ukraine

PRINCIPLES OF HUMAN-CENTRED DIGITAL JUSTICE: THE EUROPEAN APPROACH AND WAYS OF IMPLEMENTATION IN UKRAINE

Abstract. *The article is devoted to characteristics of the European approach to digital justice from the perspective of its human-centred nature and identification of the critical gaps in the implementation of the corresponding principles within the Ukrainian justice system. It outlines the two-tier normative framework of the EU, whereby the value-based guidelines, set out in the European Declaration on Digital Rights and Principles for the Digital Decade (2023), are consistently translated into functional standards in the European e-Justice Strategy 2024–2028. It is determined that the European approach is grounded in the principles of the above-mentioned Declaration, the key among them being human-centredness, solidarity and inclusion, privacy and individual control over data, a fair digital environment, and interactions with algorithms and artificial intelligence (AI) systems, etc. The article proposes a correlation between the fundamental principles of the European Declaration on Digital Rights and Principles for the Digital Decade (2023) and the substantial and operational principles in the European e-Justice Strategy 2024–2028 (access to justice, interoperability and cybersecurity, the «once-only principle», data-driven justice, etc.). The article identifies the challenges and pathways for implementing human-centred e-justice in Ukraine through the development approach applied to Unified Judicial Information and Telecommunication System (UJITS), which, despite its legal foundations in procedural legislation, remains predominantly focused on technical infrastructure. Although intended to be user-oriented*

and to enhance technical efficiency, the current UJITS Concept does not ensure adequate attention to inclusiveness (in particular, accessibility), cybersecurity, or proper data protection. It constrains the framework for data-driven justice due to the absence of structured machine-readable data (ECLI, open APIs), which hampers effective analysis of judicial practice and cross-border interoperability, and reduces the transparency of judicial data. Recommendations for harmonisation of Ukrainian legislation with the EU acquis are proposed: institutional oversight of data, structural data openness as a prerequisite for data-driven justice, and cross-border interoperability. The legislative recognition of AI in judicial processes as a high-risk system (in accordance with the EU AI Act) requires strict human oversight and fundamental-rights impact assessment, along with transparency in its use. It is emphasised that only a value-oriented transformation will enable compliance of Ukrainian legislation with the EU acquis and ensure fair, inclusive, and effective access to justice. The ***research methodology*** *incorporates the formal legal method (analysis of EU and Ukrainian normative acts), a structural-functional method (identifying the transformation of values into functional standards), the comparative-legal method (juxtaposition of EU and Ukrainian experience), and an analysis of the architecture of the UJITS.*

Keywords: *justice; digital justice; e-justice; human-centred digital transformation; principles; European Union; digital rights; protection of rights; judicial decision; national and international law; international legal standards.*

Олег Васильович Синєгубов
Національна академія правових наук України
Харків, Україна

Харківська обласна військова адміністрація
Харків, Україна

Оксана Григорівна Бортнік
Кафедра цивільного, трудового та господарського права
Харківський національний університет внутрішніх справ
Харків, Україна

Олена Михайлівна Черненко
Кафедра публічного управління, адміністрування та права
Національний університет «Полтавська політехніка імені Юрія Кондратюка»
Полтава, Україна

Кафедра права
Приватний вищий навчальний заклад «Європейський університет»
Київ, Україна

ПРИНЦИПИ ЛЮДИНОЦЕНТРИЧНОГО ЦИФРОВОГО ПРАВОСУДДЯ: ЄВРОПЕЙСЬКИЙ ПІДХІД ТА ШЛЯХИ ІМПЛЕМЕНТАЦІЇ В УКРАЇНІ

Анотація. *Статтю присвячено характеристиці європейського підходу до цифрового правосуддя з позиції його людиноцентричності та визначенню критичних прогалин у ре-*

*алізації відповідних принципів у системі правосуддя України. Окреслено дворівневу нормативну модель ЄС, у межах якої ціннісні орієнтири, закріплені в Європейській декларації цифрових прав та принципів для цифрового десятиліття (2023), послідовно трансформуються у функціональні стандарти Європейської стратегії електронного правосуддя на 2024–2028 роки. Визначено, що європейський підхід ґрунтується на принципах зазначеної Декларації, ключовими серед яких є людиноцентричність, солідарність та інклюзія, приватність і індивідуальний контроль над даними, справедливе цифрове середовище та взаємодія з алгоритмами й системами штучного інтелекту (ШІ) тощо. Запропоновано співвідношення між фундаментальними принципами Європейській декларації цифрових прав та принципів для цифрового десятиліття (2023) та сутнісними й операційними принципами Європейської стратегії електронного правосуддя на 2024–2028 роки (доступ до правосуддя, інтероперабельність та кібербезпека, принцип «одного разу», правосуддя на основі даних тощо). Визначено виклики та шляхи імплементації людиноцентричного е-правосуддя в Україні через підхід, застосований до Єдиної судової інформаційно-телекомунікаційної системи (ЄСІКС), яка, попри наявні правові засади у процесуальному законодавстві, залишається переважно орієнтованою на технічну інфраструктуру. Попри задекларовану орієнтацію на користувача та прагнення підвищення технічної ефективності, чинна Концепція ЄСІКС не забезпечує належної уваги до інклюзивності (зокрема, безбар'єрності), кібербезпеки та належного захисту даних. Вона обмежує умови для правосуддя на основі даних через відсутність структурованих машиночитуваних форматів даних (ECLI, відкритих API), що ускладнює ефективний аналіз судової практики, транскордонну інтероперабельність та знижує прозорість судових даних. Запропоновано рекомендації щодо гармонізації українського законодавства з acquis ЄС: інституційний нагляд за даними, структурна відкритість даних як передумова правосуддя на основі даних та транскордонної інтероперабельності. Законодавче закріплення статусу ШІ у сфері судочинства як високоризикової системи (відповідно до Закону ЄС про ШІ) потребує суворого людського контролю, оцінки впливу на фундаментальні права та забезпечення прозорості його використання. Наголошено, що лише ціннісно орієнтована трансформація дозволить забезпечити відповідність українського законодавства acquis ЄС і гарантувати справедливий, інклюзивний та ефективний доступ до правосуддя. **Методологія дослідження** включає формально-юридичний метод (аналіз нормативних актів ЄС та України), структурно-функціональний метод (виявлення трансформації цінностей у функціональні стандарти), порівняльно-правовий метод (зіставлення досвіду ЄС та України) та аналіз архітектури ЄСІКС.*

Ключові слова: *правосуддя; цифрове правосуддя; е-правосуддя; людиноцентрична цифрова трансформація; принципи; Європейський Союз; цифрові права; захист прав; судове рішення; національне та міжнародне право; міжнародні правові стандарти.*

INTRODUCTION

The digital transformation of justice within the European Union (EU) has acquired the character of a systemic policy that combines technological modernisation with the value imperatives of human rights protection, inclusiveness, and transparency. For Ukraine, as a candidate country for EU membership, the issue of harmonising the national e-justice system with European standards has become critically important in the context of the obligations arising from the Association Agreement between Ukraine and the

EU (2014). At the same time, the current practice of implementing the Unified Judicial Information and Telecommunication System (UJITS) in Ukraine demonstrates the predominance of a technocratic approach over a human-centred paradigm, which underscores the need for a systematic analysis of the principles of EU digital justice and the ways of their implementation.

A range of EU legal instruments on digitalisation emphasise the importance of creating a secure, interconnected, and transparent digital justice ecosystem: electronic judicial services, integrated data spaces, the development of legal technologies, and the ethical and legal regulation of artificial intelligence (AI). Particularly, 2030 Digital Compass: The European Way for the Digital Decade specifies that digital transformation must ensure modern and efficient justice systems, consumer protection, and the effectiveness of public measures, including those of law enforcement authorities (85% of criminal investigations are based on electronic evidence). What is unlawful offline is equally unlawful online; hence, law enforcement authorities must be best equipped to combat sophisticated digital crimes [1]. In line with the European Strategy for Data (2020), the establishment of sectoral and industry-specific common European data spaces for public administration bodies is envisaged. Unhindered access to EU and Member State legislation, case law, information on e-justice services, and the ability to reuse such resources are essential for the effective application of EU law and the creation of innovative «legal technologies» that support professionals (judges, state officials, corporate lawyers and attorneys) [2].

The EU Data Act (Regulation (EU) 2023/2854) emphasises that the European Data Innovation Board (EDIB) plays a key role in coordinating between competent authorities on the application of this Regulation to improve access to justice and judicial cooperation within the EU [3]. The Digital Single Market Strategy for Europe (2015) aims to support an inclusive digital market where citizens and businesses have the necessary skills to use interconnected, multilingual electronic services, including e-justice [4]. The EU Artificial Intelligence Act (Regulation (EU) 2024/1689) highlights the growing importance of AI in the field of justice. AI systems for fact analysis, legal interpretation, and alternative dispute resolution are classified as high-risk due to their potential impact on the rule of law, human rights, and the right to a fair trial. AI may support judicial activity, but cannot replace judges – final decisions must remain with humans. The classification of such systems as high-risk is set out in Annex III to this Regulation, which covers the administration of justice and democratic processes [5]. This approach is supported in academic literature, in particular: legal cases consideration, even those of minor complexity, requires the involvement of a judge capable of making an individualised legal assessment, considering all the case's circumstances. The human factor in judicial discretion remains key and cannot be replaced by AI. At the same time, e-justice technologies are appropriate for automating procedural and administrative functions, but not for making judicial decisions [6]. Ancillary functions (such as anonymisation or internal communication) are not considered high-risk. Operators of high-risk systems are required to carry out a fundamental rights impact assessment. Independent supervisory

authorities must have effective powers to conduct inspections, including access to personal data [5]. Member States are obliged to designate supervisory bodies under the General Data Protection Regulation (Regulation (EU) 2016/679) [7] or Directive (EU) 2016/680 [8]. Following the Ethics Guidelines for Trustworthy AI (2019), AI systems should not undermine the rule of law, applicable law, due process, or equality before the law [9].

Thus, the European approach to digital justice is based on a complex system of legal, ethical, and technological requirements, which poses a challenge of systemic transformation in this field for Ukraine in the context of European integration. The understanding of these challenges has intensified scholarly inquiry among domestic researchers. In particular, certain aspects of the legal foundations of the digitalisation of justice are examined by Ukrainian scholars in the context of digital transformation through the prism of European integration and human rights in the digital age [10], the European experience of digitalising executive authorities [11], the functioning of e-justice systems in European countries [12], personal data protection [13], and the information and legal framework of e-governance [14].

In the general context, O. O. Bernaziuk, in his study on the administrative and legal foundations of the use of digital technologies in law, considers e-justice as a unified, holistic and comprehensive information and telecommunication system [15, p. 24], which forms part of a broader e-governance framework. O. Z. Nykon, in a specialised study on the digitalisation of the justice system, based on a comprehensive innovative process of transformation, identifies the main challenges of e-justice in Ukraine, including the need for comprehensive modernisation of the Unified Judicial Information and Telecommunication System (UJITS), the implementation of human-centred and service-oriented approaches in e-justice, and the introduction of Artificial Intelligence (AI) under human supervision [16, p. 202–203]. The author also demonstrates the multi-level structure of the legal regulation of the digital transformation of justice in the EU [16, p. 164–189, 212], while not focusing on a detailed analysis of specific EU primary acts. D. Bohatchuk, in examining the prospects for the development of e-justice [17, p. 19], defines it as an integral element in ensuring access to justice and the rule of law, which requires the implementation of the principles of transparency, accessibility, and accountability [17, p. 33]. However, the analysis is based primarily on national legislation (in particular, the objectives set out in the Law of Ukraine «On the Judiciary and the Status of Judges») and on acts of Council of Europe institutions, notably the European Commission for the Efficiency of Justice [17, p. 19], rather than on a systematic study of the legal foundations of digital transformation in general and justice in the EU in particular. N. V. Bocharova outlines the relevant foundations and human rights-based content of the EU's digital transformation, focusing on the concept of digital humanism. This concept places people at the centre of this process, including respect for fundamental rights, the rule of law, and democracy [18].

At the same time, despite the considerable academic contribution to the field of the digitalisation of justice, a systematic analysis of the correlation and interconnection

between the principles of the European Declaration on Digital Rights and Principles for the Digital Decade (2023) and their functional embodiment in substantial and operational principles of the e-Justice Strategy 2024–2028 remains insufficiently explored. These considerations determine the relevance of a critical assessment of the implementation of the latest European standards within the Ukrainian justice system, in particular, the UJITS, from the perspective of structural data openness, interoperability, inclusiveness, cybersecurity, AI regulation, cross-border cooperation, and user experience.

The purpose of the study is to characterise the principles of human-centred digital justice of the European Union, enshrined in the European Declaration on Digital Rights and Principles for the Digital Decade (2023) and in the e-Justice Strategy for 2024–2028; to identify the patterns of transformation of general value orientations into specific functional standards and to provide a critical assessment of their implementation in Ukraine through the analysis of the functioning of the Unified Judicial Information and Telecommunication System (UJITS) and the current procedural legislation, with the formulation of recommendations to ensure full harmonisation with the EU acquis in the field under study.

1. MATERIALS AND METHODS

The methodological framework of the study consists of a set of general scientific and special legal methods of scholarly inquiry, ensuring a comprehensive analysis of the digital justice of the EU and an assessment of the state and prospects of its implementation in Ukraine. The selected methodology is aimed at identifying the structural and functional interrelations between legal values and the operational mechanisms of the digital transformation of justice, which is a necessary precondition for the development of scientifically grounded recommendations for improving legislation, institutional mechanisms and the practice of e-justice in Ukraine.

The study integrates various approaches for a systematic assessment of the principles and objectives of the digital transformation of justice, as well as for identifying its dynamics and structural-functional interconnections. The formal-legal method was applied to analyse the legal regulation of digital transformation in the EU: the European Declaration on Digital Rights and Principles for the Digital Decade (2023), which serves as a conceptual and value-based foundation; the European e-Justice Strategy for 2024–2028, which outlines the operational framework for implementation; Regulation (EU) 2024/1689 concerning the classification of AI as a high-risk system in the field of justice; as well as to examine data protection requirements and the relevant provisions of Ukrainian procedural legislation regarding electronic document management and data protection.

The structural-functional method was employed to examine the digital transformation of justice as a dynamic phenomenon. This made it possible to identify the patterns of the sequential transformation of broad digital values (such as «human-centredness» and «inclusiveness») into specific functional standards (including «data-driven justice» and the «once-only principle»); to conduct a critical analysis of the architecture and

functioning of the UJITS, comparing its technical implementation with the requirements of accessibility, cross-border interoperability and algorithmic accountability; and to distinguish between the formally enshrined human-centredness (in the UJITS Concept) and the actual state of digital justice (its technical infrastructure), which made it possible to substantiate the conclusion that the model of managerial and technical efficiency prevails over the value-oriented model.

The comparative legal method was applied to correlate the legal regulation of e-justice in the EU and Ukraine, which made it possible to identify national challenges related to accessibility, data-driven justice and AI regulation, and to determine the most relevant vectors of harmonisation for a candidate country for EU membership.

The chosen methodology has ensured the formulation of legislative and institutional recommendations for addressing existing gaps and identifying directions for the successful harmonisation of the Ukrainian justice system with the standards of the EU acquis.

2. RESULTS AND DISCUSSION

2.1. Principles of the European Declaration on Digital Rights and Principles for the Digital Decade in the Context of Digital Justice

The approach to building a resilient digital justice system in the context of access to justice in the digital era must take into account the principles set out in the European Declaration on Digital Rights and Principles for the Digital Decade (2023) [19]. Their content is examined below concerning the digitalisation of justice within the EU.

1. *The principle of «Putting people at the centre of the digital transformation»* shapes a human-centred paradigm in which digital technologies are instrumental and serve to strengthen human rights, democracy, and the rule of law. In the field of justice, this entails the introduction of digital solutions that take into account the rights and needs of all users, particularly vulnerable groups. The EU legal framework imposes obligations to guarantee rights in both online and offline environments, to ensure the accountability of digital actors, and to uphold accessibility, non-discrimination, and legal certainty. The human being remains the ultimate decision-maker even where AI is deployed. This principle constitutes both an ethical and a legal requirement: the digitalisation of judicial proceedings must promote human rights and access to justice, while limiting technological intervention through value-driven safeguards [19]. In current legal scholarship, the horizontal application of the rights guaranteed by the Charter of Fundamental Rights of the European Union [20] is regarded as a mechanism for addressing deficits in the implementation of the rule of law in the digital environment. Such an approach strengthens the legal protection of individuals in their relations with large digital platforms and online service providers [21].

2. *The principle of «Solidarity and inclusion»* shapes a socially oriented paradigm for justice digitalisation, which must be both technically efficient and socially just, inclusive, and non-discriminatory. It necessitates ensuring the accessibility of digital justice services for all, including persons with disabilities, women, and residents of rural

and remote areas. The requirement to «leave no one behind» directly aligns with the right to equal access to justice, as enshrined in the Charter of Fundamental Rights of the European Union [20], the UN Convention on the Rights of Persons with Disabilities [22], and the EU Gender Equality Strategy 2020–2025 and the EU Strategy for the Rights of Persons with Disabilities 2021–2030 [24; 25]. It is necessary to implement inclusive information and communication technology (ICT) solutions, incorporating alternative offline formats and digital assistance tools. All stages of transformation, in addition to efficiency, must be aimed at realising fundamental rights, notably the rights to a fair trial and non-discrimination. Particular attention must be paid to overcoming digital barriers faced by women and ensuring safe access for victims of gender-based violence. «Solidarity and Inclusion» is becoming the legal standard for socially responsive and rights-compliant digital justice [19].

In the context of inclusion, two key EU strategies are worth noting. Thus, the Strategy for the Rights of Persons with Disabilities 2021–2030 defines that persons with disabilities in most countries have limited access to inclusive basic services, including justice, despite having the right to equal opportunities, protection from discrimination, and freedom from violence. A separate point is devoted to improving access to justice through the provision of reasonable accommodation. However, both practical and legal barriers continue to hinder the full participation of persons with disabilities in judicial proceedings and holding professional roles within the justice system (including judges, attorneys, prosecutors), especially for those with intellectual disabilities, psychosocial impairments, or mental health conditions. The European Commission has committed to providing Member States with guidance on access to justice for persons with disabilities and to support their participation as professionals within the justice. Within the framework of the professional training strategy, the Commission will focus on the protection of rights in the digital environment, in particular the relevant provisions of EU law and the UN Convention on the Rights of Persons with Disabilities. These commitments are grounded in international recommendations, including those of the UN [23], and are aimed at collecting best practices on supported decision-making [24].

The EU Gender Equality Strategy 2020–2025 states that women with health conditions or disabilities are more likely to be victims of various forms of violence. It emphasises the development and funding of measures to combat abuse, violence, forced sterilisation, and forced abortion, through capacity-building for professionals and awareness-raising campaigns on rights and access to justice. Effective violence prevention requires an interdisciplinary approach involving a range of services, including the criminal justice system, victim support services, and social and healthcare services [25]. It is a well-founded view that the digitalisation of justice should be considered a driver for improving access to justice, particularly for women, who are often the primary carers within families, as online formats can help to reduce time and logistical barriers, as well as the risk of psychological discomfort and intimidation, which may be associated with traditional court hearings [26].

3. *The principle of «Connectivity»* recognises digital infrastructure as a key precondition for the realisation of human rights in the digital age, and affirms that without high-quality, stable, and non-discriminatory access to the Internet, the digitalisation of justice is unattainable. High-speed connectivity determines procedural equality: limited Internet access deprives certain groups – including residents of rural areas and persons with low income – of the ability to make effective use of digital justice services and legal aid. Reliable connectivity is equally essential for the effective functioning of justice at the transnational level. Openness and neutrality of the net prevent censorship and ensure equal access to legal information. Within justice, the principle of connectivity constitutes an instrumental guarantee of access to justice and reinforces the legitimacy of digital transformation through equality, openness, and technological fairness [19].

4. *The principle of «Digital education, training and skills»* recognises knowledge and competencies as key prerequisites for the realisation of rights in the digital environment. In the field of justice, this means that participation in digital forms of judicial proceedings – such as e-courts, video hearings, and online submission of claims – requires the ability to use digital tools effectively and autonomously. The absence of digital skills constitutes a factor of hidden discrimination, especially against older persons, women, persons with disabilities, and socially vulnerable groups. Digital literacy is directly linked to the right to access to justice, and the implementation of ICT solutions necessitates the development of digital competences within the professional environment – including judges, prosecutors, attorneys, and court administration staff. Media literacy and critical thinking are fundamental for navigating digital procedures, assessing legal information online, and countering fraudulent legal services. This principle underpins the cognitive foundation of the digital transformation of justice as an indispensable condition for the realisation of rights [19].

5. *The principle of «Fair and just working conditions»* establishes the ethical and legal guidelines for digitalisation within the professional environment. Digital transformation – including the deployment of e-courts, AI, video hearings, and electronic e-document management – reshapes working conditions, thereby necessitating additional guarantees: maintaining work – life balance; addressing the psycho-emotional workload linked to digital formats; protecting privacy and preventing digital monitoring, particularly in remote working arrangements; ensuring transparency in the use of AI and carrying out risk assessments of its impact on proceedings; and guaranteeing the mandatory involvement of human decision-making. Non-compliance with these standards risks undermining judicial independence and diminishing the quality of justice. The participation of professional associations – including those representing judges, attorneys, and court administrators – in developing ethical frameworks for digitalisation is essential to ensure legitimacy in the transformation process. This principle serves to safeguard human dignity and ethical standards in the digital age, ensuring an appropriate balance between the efficiency of digital tools and the rights of justice professionals [19]. In this regard, the observation made by Onțanu E. A. is particularly pertinent: judicial independence is of critical importance in the context of the digitalisation of justice,

as technological integration may create risks for judicial discretion. To address such risks, it is advisable to involve technical experts in the development of ICT solutions and to introduce procedures for the detection of coding errors and digital vulnerabilities, thereby enhancing the effectiveness of digital governance in the field of justice [27].

6. *The principle of «Digital public services online»* positions justice as an integral component of e-government. E-justice encompasses the online submission of documents, remote participation in hearings, electronic delivery of judgments, authentication, system interoperability, and cross-border access. A unified digital identity in the judicial context ensures simplified access to e-courts, secure communication, and the legal validity of electronic actions. The «once-only principle» enables the automated retrieval of certain data (for example, from official registers), thereby enhancing the efficiency of proceedings. Cross-border interoperability constitutes the foundation for cross-border judicial proceedings, the operation of the e-Justice Portal, and the mutual recognition of judgments within the EU. This principle shapes the vision of digital justice within an accessible, secure, and user-centred digital citizenship infrastructure. Public digital services require technical compatibility, data protection, and the legal recognition of electronic actions [19].

7. *The principle of «Interactions with algorithms and artificial intelligence systems»* sets out the requirements for the use of AI: technologies must remain under human control and comply with the standards of human rights, non-discrimination, and due process of law. This is of critical importance in the field of justice, as algorithmic decisions may affect an individual's procedural status and, more broadly, their life prospects. Automatic case routing, recidivism prediction, automated decisions in minor cases, and big data analytics require strict ethical and legal regulation. Interaction with AI must be accompanied by informed consent, an explanation of the system's operating principles, and the right to human review, which means ensuring human control in decision-making, evidence assessment, and specified legal consequences. This principle guards against the discriminatory potential of algorithms trained on biased data and requires that AI not circumvent an individual's autonomous will by substituting their choice. Emphasis is placed on the need for safeguards, including auditing, transparency, accountability, and verification of AI decisions before their application in judicial practice. The principle regulated the limits of human-centred digital justice, where AI performs an auxiliary function, enhancing efficiency while ensuring guarantees of a fair trial and the freedom of choice [19]. As noted by Depasquale F., by 2034, AI is expected to be actively integrated into judicial practice for resolving standardised cases, with the anticipated benefits of improving the consistency of judicial decisions and reducing the impact of human bias. At the same time, a critical challenge arises in safeguarding impartiality and preserving judicial independence under increasing algorithmic influence [28].

8. *The principle of a «A fair digital environment»* establishes the ethical and legal foundations for a digital environment in which individuals are not merely protected subjects but autonomous agents of choice. In the field of justice, this means that digital

services, including AI systems, must be based on transparency, openness, and non-discrimination. According to paragraph 10, users must be granted access to information regarding the application of digital tools and their potential impact on legal proceedings. Algorithmic decisions must be intelligible, reasoned, and safeguarded against manipulation. Subparagraph (11a) guarantees the right to an alternative: access to justice cannot be limited solely to digital channels, particularly for vulnerable individuals. The risks of monopolisation of digital platforms may undermine the neutrality and equality of legal access. Paragraph 11 ensures a level playing field for all e-justice service providers, including small law firms and non-governmental organisations, thereby promoting innovation and user-orientation. Subparagraph (11b) highlights the importance of interoperability and open technologies that enable cross-border cooperation between EU Member States (notably via e-CODEX), while reducing dependence on private and opaque platforms. This principle thus establishes institutional guarantees ensuring that digital justice remains a public good – protected from technocratic monopolisation and focused on individual rights and freedom of choice [19].

9. *The principle of «Participation in the digital public space»* underscores the significance of the digital environment as a space for exercising democratic rights, particularly access to justice, freedom of information, and participation in legal discourse. Digital justice is conceptualised as an integral component of an open public space that interacts with digital communication channels, information dissemination, and public control. According to paragraph 12, digital justice should ensure multilingual access to judicial information, legal norms, and procedures via open online resources, which is a critical factor for migrants, refugees, and national minorities. Paragraph 13 establishes the limits for the judiciary's impact on freedom of expression, highlighting the need to strike a balance between protection from illegal content (such as defamation or cyberbullying) and respect for freedom of speech. Paragraph 15 draws attention to the influence of digital platforms on the perception of justice: social media, blogs, and podcasts are becoming platforms for appeals against court decisions, so the system of justice must ensure the protection of trial participants against manipulation and hate speech, alongside the development of institutional digital communication channels. Subparagraph 15(d) emphasises the importance of creating a secure environment free from disinformation, cyberattacks, and online violence directed at witnesses, judges, or victims. Participation in the digital public sphere constitutes an essential element of access to justice. Digital justice must remain open, secure, and integrated within the democratic online discourse, with particular attention to vulnerable groups and the standards of freedom of expression [1].

10. *The principle of «A protected, safe and secure digital environment»* requires that access to electronic judicial services and communications be ensured following the principles of confidentiality, integrity, availability, and authenticity of information. Digital justice tools must guarantee the protection of personal data (through encryption, authentication mechanisms, and the prevention of unauthorised access) as a prerequisite for upholding the right to privacy. The reliability and continuity of judicial platforms

are key to ensuring access to justice. This includes the verification of the integrity of digital evidence and documents, protection against cybersecurity threats, and the ability to respond effectively to incidents. The principle also entails responsibility for the dissemination of harmful or discriminatory content and guarantees access to justice in the context of digitalisation through the development of technological and legal infrastructure and resilient e-justice ecosystem [19].

11. *The principle of «Privacy and individual control over data»* defines the normative framework for ensuring informational autonomy of the individual. In the field of digital justice, this principle manifests across several dimensions: security of digital communication channels (including electronic submissions, online hearings, and video conferencing), robust authentication mechanisms, and the application of data protection by design and by default, as stipulated by EU legislation; the right to personal data encompasses the issues of access to information, the ability to restrict its dissemination, and the exercise of the right to be forgotten, particularly in cases involving sensitive issues such as discrimination, violence, or medical circumstances; digital inheritance concerns the procedural representation of an individual's interests after death and the submission of digital evidence in relevant proceedings; guarantees against digital surveillance, unauthorised recordings, hacker intrusions, excessive data analytics, and external pressure, particularly in publicly sensitive cases. Therefore, this principle establishes the limits of permissible personal data processing in digital justice, defining standards of information security, digital dignity, and procedural autonomy of the individual, ensuring legal predictability within the digital environment, and maintaining trust in the justice [19].

12. *The principle of «Protection and empowerment of children and young people in the digital environment»* promotes a digital environment that is sensitive to the age-specific needs of minors. In digital justice, this principle aims to raise the standards of protection for children and serves as a benchmark for designing digital services tailored to young users. Children's access to digital judicial procedures requires special architectural design of interfaces, clear communication, and technologically facilitated support mechanisms (e.g., digital mediation or representation). Cases involving cybercrime against children require special attention, as digital traces must be processed with strict confidentiality, while digital interviewing practices must adhere to standards for preventing secondary victimisation. The digital transformation of the judiciary must be accompanied by the development of legal awareness infrastructure for children and young people, including specialised online resources, educational products, and the integration of digital legal literacy into media education curricula. Moreover, the principle calls for the inclusion of young people in shaping digital justice policy through participatory mechanisms such as advisory councils. In this way, the principle outlines the age-sensitive nature of digital justice, requiring the integration of confidential, participatory, and age-appropriate approaches to ensure procedural security of children [19]. This principle is further embedded in the norm of ensuring the best interests of the child within the digital environment. It functions as a guiding reference for policymaking

in the fields of child rights, development, and well-being. European standards underline the necessity of observing the principles of proportionality and non-discrimination when assessing such interests in digital contexts [29].

13. *The principle of «Sustainability»*, understood as a requirement of environmental responsibility in the digital transformation of justice, implies that the design, implementation, and use of digital tools must take into account ecological impact, resource efficiency, and long-term viability. The digitalisation of justice cannot remain detached from the context of the European Green Dea [30] and the Sustainable Development Goals (SDGs) [31], as the legal system not only reflects but also shapes state behaviour. Digital judicial infrastructures must comply with environmental sustainability requirements through energy-efficient data centres and repairable hardware and software solutions. Digitisation reduces the material footprint, but inefficient design can increase energy consumption and digital waste. According to the Declaration, users of digital judicial services should be informed about the platform's energy consumption, technical viability, and updateability. The state is obliged to implement environmentally conscious digital justice policies by selecting sustainable service providers and adopting green IT procedures. The principle outlines the obligations of judicial institutions regarding the minimisation of e-waste, the introduction of eco-labelling, and the promotion of energy-saving technologies. Ultimately, this principle transforms the digital modernisation of justice into an ethical and ecological paradigm, where digitalisation becomes a mechanism of resource justice and institutional responsibility [19].

The analysis of the Declaration's principles in the context of digital justice demonstrates that the digital transformation of justice within the EU extends far beyond technical modernisation. It is firmly grounded in a value-based and legal framework that safeguards fundamental human rights, inclusivity, ethics, and sustainability. The principles of human-centredness, inclusion, privacy, security, participation in the digital public space, and sustainability, etc. establish a multidimensional normative framework for the digitalisation of justice, defining the obligations of both the EU and its Member States to ensure equal, secure, and effective access to justice in the digital age, with particular attention to vulnerable groups, transparency of AI-driven decisions, environmental responsibility, and technological fairness. Digital justice in the EU is evolving into a comprehensive legal ecosystem that integrates technological innovation with the foundational principles of democracy, human rights, and sustainable development.

2.2. Correlation Between the European Declaration on Digital Rights for the Digital Decade and the European E-Justice Strategy 2024–2028 Principles

The principles set out in the European Declaration on Digital Rights and Principles for the Digital Decade (2023) outline the general directions of digital transformation within the EU. In turn, the specific principles established in the European e-Justice Strategy 2024–2028 are categorised into substantial and operational principles [32].

The substantial principles include:

– *the principle of «Respect for fundamental rights and principles»* establishes that the digital transformation of justice must be carried out with unconditional respect for fundamental rights, judicial independence, and the rule of law. Particular attention should be paid to criminal proceedings, where the use of remote technologies must not compromise the right to a fair trial, the physical presence of the individual during proceedings, or the right to defence. It also requires safeguards against cyber threats, the prevention of digital inequality and discriminatory effects arising from biased algorithms;

– *the principle of «Access to justice»* stipulates that further technological solutions have significant potential to expand and enhance access to justice within the EU, particularly in the context of low-risk tasks where algorithmic tools can effectively support both citizens and judicial authorities. Legal scholarship supports the view that accessibility is a key criterion for the effective functioning of e-justice, providing equal access to digital judicial services, their technological interoperability, linguistic inclusivity, intuitive design, the absence of financial barriers, and the need to improve the digital literacy of the population [33];

– *the principle of «People centricity»*, in the context of the digitalisation of justice, refers to accessibility and inclusiveness, particularly for individuals lacking digital skills. The reorientation of judicial systems towards the needs of users is expected to enhance trust in institutions, strengthen the legitimacy of digital transformation, and improve the overall efficiency of judicial proceedings$

– *the principle of «Bridging the digital divide»* is a crucial prerequisite for ensuring equal access to justice across the EU. It addresses drivers of social exclusion and barriers to the realisation of human rights. Harmonising the level and inclusivity of digitalisation among the judicial systems of Member States through the exchange of best practices will contribute to a fair and equitable digital transformation of justice;

– *the principle of «Digital empowerment of users»*, with particular emphasis on the upskilling of professionals, facilitates effective navigation within both national and European legal systems and contributes to enhanced legal coherence;

– *the principle of «Sustainability»* requires that every e-Justice service should be implemented and maintained sustainably, entailing predictability in terms of its long-term economic, environmental, and social impact [32].

The operational principles include:

– *the «Once-only principle»* in the provision of judicial services aims to minimise procedural duplication and reduce the administrative burden on individuals by reusing relevant information that has already been entered into the system. Its implementation must strictly respect the right to privacy and the right to be forgotten;

– *the principle of «Digital by default»* entails the reorientation of justice services towards digital formats as the primary mode of delivery. This facilitates procedural simplification, reduces reliance on paper-based documentation, and enhances the efficiency of judicial processes. At the same time, non-digital alternatives must remain

available to ensure access to justice for individuals not encompassed by digital technologies;

– *the principle of «Interoperability and cybersecurity»* stipulates that ensuring interoperability between judicial systems is a key prerequisite for the effective exchange of data and coordination between legal institutions across EU Member States. This contributes to the coordination of actions, overcoming barriers between national legal systems and enhancing the consistency of justice in the EU;

– *the principle of «Dynamic justice»* asserts that justice must be flexible and capable of adapting to the evolving needs of society. Considering individual circumstances, users' capacities and competencies, as well as effective change management, fosters the development of a more resilient and responsive justice system. Digital technologies and data play a central role in this process. The integration of digitalisation, data analytics, and artificial intelligence into the operation of judicial institutions increases their efficiency;

– *the principle of «Data-driven justice»* establishes that decision-making processes must be grounded in reliable and verifiable data. Accordingly, digital justice initiatives should incorporate the systematic collection, analysis, and utilisation of data as a foundation for effective governance and risk mitigation, particularly concerning technological and statistical biases. Enhancing transparency within the judicial system fosters greater public trust in justice. Open access to judicial data empowers both citizens and businesses to engage in self-directed dispute resolution and supports evidence-based policymaking. This approach also facilitates the emergence of new innovative initiatives and inter-institutional synergies. Crucially, such processes must ensure the proper protection of personal data and uphold high standards of cybersecurity;

– *the principle of «Open-source»* emphasises the importance of using open source software while ensuring adequate data protection. The benefits of this approach – including cost reduction, the promotion of innovation, and improved transparency – are particularly valuable for the justice sector. Such solutions also contribute to accountability and strengthen trust in judicial and law enforcement bodies [32].

The European Declaration on Digital Rights and Principles for the Digital Decade (2023) establishes a value-based and legal framework for digital transformation, encompassing all spheres of public life and setting general benchmarks for digital policy. The European e-Justice Strategy 2024–2028 particularises these foundations through substantial and operational principles aimed at the practical implementation of the digital modernisation of justice within the EU. The correlation between these documents enables tracking the transformation of general digital values into functional standards of justice, ensuring the efficiency, accessibility, security, and transparency of e-justice. Therefore, the general principle of «putting people at the centre of digital transformation» is specified in the e-Justice Strategy through the concepts of people centricity (inclusiveness, accessibility, and user-orientation) and dynamic justice (adaptability to individual needs). Bridging the digital divide is a functional continuation of the general principle of «solidarity and inclusion», focusing on technological inequality, while the special

principle «digital by default» approach reflects the need to accommodate diverse user interests through digital services with offer alternative formats. The principle of «digital education, training and skills» continues in such special principles enshrined in the e-Justice Strategy as «digital empowerment of users», which emphasizes digital preparedness, including the professional development of justice sector professionals, and the principle of dynamic justice, which takes into account users' levels of digital literacy. The ecological imperative laid out in the Declaration continues in the principle of sustainability in the e-Justice Strategy. It is also reflected in the special principle of «open source», which promotes reduced reliance on resource-intensive commercial solutions. The general principle of «participation in the digital public space» in the Declaration is realised through the principle of «access to justice» by means of deploying electronic tools and the «once-only principle», which directly reflects the requirements of digital service infrastructure. The principle of «interactions with algorithms and AI systems» is concretised through the principles of «data-driven justice» and «dynamic justice» in the e-Justice Strategy, with clear stipulations regarding AI use – transparency, auditability, and the avoidance of bias. The principle of «privacy and individual control over data» is a foundational condition for the implementation of all specialised principles, demonstrating the integrated presence of privacy within the digital transformation of justice, and aligning with the substantial principle of «respect for fundamental rights and principles». The correlation between the general principles of the Declaration and the specific principles of the e-Justice Strategy reflects a coherent and consistent model for the digital transformation of justice in the EU. While the general principles serve as a normative and value-based foundation, the specific principles provide operational and functional dimensions, translating broad approaches into practical mechanisms. This dual-level framework ensures a balance between the EU's legal values and technological modernisation, thereby contributing to the provision of effective, secure, and inclusive access to justice in the digital age.

2.3. Digital Transformation of Justice in Ukraine: Progress, Challenges and Compliance with the Principles of Digital Justice in the EU

On the basis of the Association Agreement between Ukraine and the European Union (2014), Ukraine has been gradually adapting its national legislation to the EU acquis in the field of digital transformation, of which the digitalisation of justice is an integral component [34]. According to the report, it has been determined that alignment with European standards is required in the areas of electronic identification, cross-border data exchange, digital public services and e-governance [35], which constitute an important foundation for e-justice in accordance with EU principles. Access to justice through digital means necessitates changes and improvements in the legal, technical, and organisational conditions related to the submission and assessment of electronic evidence, compliance with IT standards within the e-justice system, the development of training in the field of e-governance, and the enhancement of citizens' digital literacy [36].

Ukraine has enshrined in the «Roadmap on the rule of law» (2025) specific commitments regarding the comprehensive digital transformation of the judicial system and the protection of personal data in accordance with European standards. In particular, by the fourth quarter of 2025, national legislation must be fully aligned with the key European acts – the General Data Protection Regulation (GDPR), Directive 2016/680, and the modernised Council of Europe Convention No. 108. Furthermore, by the end of 2026, a National Commission on Personal Data Protection and Access to Public Information is to be established as an independent supervisory authority with enforcement powers, in compliance with GDPR requirements, to ensure effective oversight of data processing standards in the digital environment. The digitalisation of justice involves a systemic modernisation of judicial infrastructure in line with the European e-Justice Strategy for 2024–2028. By the second quarter of 2025, a Concept and Roadmap for IT solutions in the judicial system are to be developed, clearly defining sources of funding and institutional responsibilities. The technological transformation includes the creation of an integrated document management subsystem with centralised automatic case allocation, a unified personalised space for participants in judicial proceedings, and interoperability with pre-trial investigation systems such as «СМЕРЕКА» (management system for investigations, escalation, control and analysis) and «іКейс» (information and telecommunication system of pre-trial investigation) [37]. These measures demonstrate the intention to establish a reliable technological foundation for integrating the national judicial system into the European digital legal space.

At the current stage, the development of e-justice in Ukraine in line with European standards depends primarily on the legal regulation and modernisation of the UJICS, as well as the implementation of the relevant legal and technological European standards. According to the latest data from the State Judicial Administration, the reconstruction of 12 subsystems of the UJICS is planned by 2029 [38].

An assessment of the state of justice digitalisation in Ukraine, the Regulation on the Procedure for the Functioning of Certain Subsystems (Modules) of the Unified Judicial Information and Telecommunication System (the Regulation on the UJITS) [39], and the UJITS Concept [40], viewed through the prism of the principles of the European Declaration on Digital Rights and Principles for the Digital Decade (2023) and the European e-Justice Strategy 2024–2028, makes it possible to identify both progressive steps and difficulties in the implementation of human-centred digital justice. The Regulation on the UJITS primarily confirms a model of administrative efficiency and automation of internal court processes (para. 3), which results in certain fundamental shortcomings. In particular, the Regulation on the UJITS does not contain requirements for inclusiveness (accessibility) and does not contribute to data-driven justice, as it lacks provisions on structured data or the European Case Law Identifier (ECLI) necessary for judicial data transparency. Moreover, the Regulation on the UJITS restricts users' rights (paras. 21, 46), placing upon them the risks associated with the technical impossibility of participation (for example, interruption of videoconferencing), which contradicts human-centred standards.

The principle of «Putting people at the centre of the digital transformation» implies that digital technologies are instrumental and serve to strengthen human rights, democracy, and the rule of law. The UJITS Concept recognises human-centredness as one of the key principles of system design, defining that the needs and interests of users, as well as the convenience and intuitiveness of user interfaces, should be prioritised in the design and development of the system [40, p. 14]. The technical audit of the UJITS (2023–2024) demonstrated that the system was built primarily as a technological infrastructure rather than as an ecosystem oriented towards the needs of various categories of users. The fragmentation of services among subsystems forces users to adapt to the technical logic of the system instead of the system adapting to their needs. The current state of the UJITS indicates a significant gap between the declared human-centredness and the actual compliance of the technological infrastructure. The absence of up-to-date technical documentation, complex and non-intuitive user interfaces, and violations of accessibility principles prevent citizens from having full access to digital justice [40, p. 8–10]. Particularly critical issues include the lack of critical infrastructure redundancy, gaps in information security, and the use of heterogeneous software without proper standardisation. Such limited functionality of subsystems, combined with gaps in legal regulation, hinders effective digitalisation. The absence of a systematic quality monitoring mechanism distances the Ukrainian judicial system from the European standards of digital justice, where technologies genuinely serve to reinforce human rights and ensure access to justice.

The principle of «Solidarity and inclusion» places particular emphasis on the requirement to «leave no one behind», which is operationalised in the EU through the Strategy for the Rights of Persons with Disabilities 2021–2030 and the Gender Equality Strategy 2020–2025. The UJITS Concept sets out the principle of accessibility and inclusiveness, requiring the system to comply with DSTU EN 301 549:2022 «Information technologies. Accessibility requirements for ICT products and services». At the same time, the system audit recorded non-compliance with accessibility principles, which renders equal access to digital justice impossible for vulnerable groups of the population [40, pp. 10, 14]. Adaptive interfaces for persons with visual impairments and specialised functions for persons with hearing impairments are absent. Gender inclusiveness also remains problematic: the UJITS Concept does not provide for dedicated secure communication channels for victims of gender-based violence, which contradicts European requirements on ensuring safe access for victims of violence. The mobile application «Court in a Smartphone», which was intended to ensure access to justice via a smartphone, is characterised by technical instability, as evidenced by numerous user complaints [40, p. 6; 41].

The principle of «Digital education, training and skills» recognises knowledge and skills as key prerequisites for exercising rights in the digital environment. Educational measures and the enhancement of digital literacy among citizens and civil servants are essential for ensuring effective judicial proceedings and access to digital justice, overcoming the digital divide between different population groups, and fostering trust

in electronic judicial services. The UJITS Concept acknowledges this challenge by including a «Training Management» subsystem within the system architecture [40, p. 34–35]. Persistent problems with user experience [40, p. 10] also create a risk of a digital divide. European practice demonstrates that investment in digital literacy is no less important than the development of technical infrastructure, as competent users are those capable of realising the potential of the digital transformation of justice and ensuring its human-centred nature in practice.

The approach to regulating the use of AI in the judicial system of Ukraine remains fragmented and insufficiently consistent. The Concept for the Development of AI (2020) outlines general objectives and refers to the Ethical Charter on the Use of AI in Judicial Systems and their Environment of the European Commission for the Efficiency of Justice [42]. The current Action Plan based on the Concept for the Development of AI assigns the Ministry of Digital Transformation the obligation to develop and submit to the Cabinet of Ministers of Ukraine, by the fourth quarter of 2026, a draft law on the legal regulation of AI development [43]. At present, the above-mentioned Plan does not provide for a more detailed regulatory framework.

Regarding current legislation, the Code of Judicial Ethics provides that the use of AI by a judge is permissible, provided that judicial independence and impartiality are maintained, and that such use does not concern the assessment of evidence or the decision-making process [44, Art. 16]. The UJITS Concept defines the directions and limits of AI application, establishing an exclusively assistive role with a specific list of permitted operations. The main domains of AI use include document processing, automatic classification, legal entity recognition, data anonymisation, summarisation of document content, and the generation of concise summaries. Functionality may include a virtual assistant-avatar for basic legal support, drafting of document templates, recommendations on case-handling methodology, selection of optimal models based on analysis of similar cases, retrieval of case-law, verification of the relevance of legislation, and detection of procedural anomalies (such as disregarding the case context, evidence, or deviations from established practice). Language technologies will provide speech-to-text for hearing transcription and text-to-speech for inclusiveness of persons with visual impairments [40, p. 24–25, 42–43, 46–47]. The Ukrainian approach corresponds to the European approach to AI self-learning [40, p. 43]. At the same time, an assessment of the impact on fundamental rights, as required by the EU Cybersecurity Act (2019), is necessary, as well as the establishment of independent supervisory bodies with effective powers to conduct independent supervisory audits and compliance assessments.

With regard to personal data protection and cybersecurity, the principle of «Privacy and individual control over data» is implemented through the requirements of procedural legislation concerning qualified electronic signatures (QES) and the comprehensive information security system, in particular through user authentication and authorisation using QES tools. The UJITS Concept provides for the establishment of information security measures, multi-factor authentication, monitoring of information-security

events, secure data exchange, protection of information integrity, protection of transaction authenticity, protection of transaction privacy, protection of information from modification, and other safeguards [40, p. 19–20]. At the same time, the practical overall level of cybersecurity of the judicial infrastructure requires strengthening due to the absence of a systematic approach to information-security matters, including reservations at the level of data centres, server, and network equipment [40, p. 10]. Under conditions of martial law and heightened cyber threats, these deficiencies pose significant risks to the functioning of the judicial system.

Transparency and openness of data, as derived from the principle of «Data-driven justice», require structured metadata and machine-readable standards. In particular, the UJITS Concept provides for the creation of an updated subsystem of the Unified State Register of Court Decisions (USRCD) with enhanced analytical and AI tools, including contextual search for relevant documents [40, p. 27–28, 45]. At the same time, the transition to digital justice is not limited to the digitisation of paper documents. It requires a transformation that ensures openness, interoperability, and the capacity to analyse large datasets. To comply with the European approach to data-driven justice, it is necessary to ensure: structured data formats (XML/JSON) – that is, a shift from free-text documents to standardised, machine-readable data formats as a basis for automated information exchange between systems; the ability to generate and export a complete set of standard data (metadata) on judicial decisions as a prerequisite for effective analysis, statistics, and data-driven policy-making; mandatory tagging of elements in judgments (for example, markup for case identifiers, cited provisions, and the operative part), which converts a judgment into a structured dataset suitable for AI processing and precise legal analytics; implementation of the European Case Law Identifier (ECLI) to support international interoperability of judicial data; provision of open Application Programming Interfaces (APIs) enabling external automated systems (including legal-tech companies, researchers, and other stakeholders) to obtain judicial decisions and related data automatically and in a structured format (XML/JSON). The absence of these structural elements makes it impossible to conduct effective large-scale data analysis, develop legal technologies, and create legal analytics tools, which constitutes a major obstacle to achieving data-driven justice.

With regard to the legal regulation of e-justice in Ukraine, the procedural legislation of Ukraine (for example, Article 6 of the Commercial Procedure Code [45], Article 35 of the Criminal Procedure Code [46], and Article 14 of the Civil Procedure Code [47]) establishes a unified technological framework. This includes, in particular: automated allocation of cases to judges based on the principles of randomness and balanced workload; mandatory registration of all procedural documents in the UJITS on the day of receipt; basic functionality for electronic exchange of documents between the court and participants in proceedings; the conduct of hearings via videoconference; and electronic user accounts for accessing case materials. Technical requirements are determined by the use of QES and an information security system with confirmed compliance. The legal regime governing the use of electronic user accounts provides

for mandatory registration for advocates, notaries, private enforcement officers, forensic experts, state authorities, local self-government bodies, and legal entities, while registration remains voluntary for other individuals (reflecting the European «Digital by default» principle with alternative access channels). Electronic service of documents is ensured for users with an electronic account. Paper and electronic document workflows currently operate in parallel. However, the implementation of the «Once-only principle» remains problematic. Despite integration of UJITS with state registers, users are frequently required to submit the same information repeatedly due to technical limitations in inter-system interoperability. The mixed document workflow (established, in particular, by Part 8 of Article 14 of the Civil Procedure Code) functions as a transitional mechanism but, in practice, results in duplication of processes.

Thus, the procedural legislation and the Regulation on the UJITS establish an initial legal framework for the digitalisation of justice in its technological dimension; however, neither the UJITS Concept nor the existing normative acts currently demonstrate a value-oriented approach. In view of the principles of human-centred digital justice, the technical modernisation of the organisation and functioning of the judiciary in Ukraine should be understood as a value-driven transformation. It is critically important that the reform be grounded in the principles of human-centredness, inclusiveness, and data transparency.

CONCLUSIONS

The European approach to the digital transformation of justice is characterised by coherence and a clearly structured framework. The value-based layer is embodied in the European Declaration on Digital Rights and Principles for the Digital Decade (2023), which establishes general principles, among which those most significant for the justice sector include human-centredness, solidarity and inclusion, privacy and individual control over data, a fair digital environment, and interactions with algorithms and AI systems, etc. These value-oriented requirements for digital transformation are to be implemented through an operational layer, which is articulated in the European Strategy for e-Justice 2024–2028 through substantial principles (respect for fundamental rights and principles, access to justice, People centricity, bridging the digital divide, digital empowerment of users, and sustainability) and operational principles (the «once-only principle», «digital-by-default», interoperability and cybersecurity, dynamic justice, data-driven justice, and open-source principle).

A regular pattern has been identified whereby the values of human-centredness and inclusiveness undergo a sequential transformation into specific functional requirements (data-driven justice, the «once-only principle», accessibility, open APIs, ECLI). This mechanism ensures an optimal balance between fundamental rights and technological implementation: the overarching principle of «putting people at the centre of digital transformation» is operationalised through user-centric system design; the principle of «solidarity and inclusion» is implemented through the bridging of the digital divide and adherence to accessibility standards; and the principle of «interactions with algorithms and AI systems» is realised through data-driven justice with mandatory human control.

The analysis of EU normative documents regulating digital transformation demonstrates that digital rights must be embedded within the architecture of judicial systems. The digital transformation of justice in the European model establishes a new standard that combines technological efficiency (speed and automation of processes) with legal safeguards (ensuring information security and data integrity), innovation (deployment of AI and new services) with inclusiveness and accessibility (priority to user needs, compliance with accessibility standards), and automation (use of AI for assistance) with human oversight (a subsidiary role for technology, AI exclusively as an assistant).The European approach to the digital transformation of justice illustrates a clear systemic shift from merely removing barriers to actively harnessing opportunities, including digital education, technical support, intuitive interfaces, ensuring structural openness and data interoperability, as well as transitioning to human-centred design. Technologies, while a critical element of judicial systems, play only a subsidiary role, without replacing humans and their judgments, ensuring transparency of automated processes, guaranteeing non-discrimination and legal safeguards for all participants, and maintaining mandatory human control at decision-making stages.

The analysis of procedural legislation and the functioning of the UJITS demonstrates that the existing model of e-justice in Ukraine (regulated by the Commercial Procedural Code, Civil Procedural Code, Code of Administrative Procedure, and Criminal Procedural Code) is centred on electronic document flow and automated case allocation, yet lags behind European standards on security, data protection, inclusiveness, and systemic integration. It retains the predominance of paper case files, does not require structural data openness, and remains technologically fragmented. Significant gaps have been identified between the declared human-centred approach and its practical implementation, as UJITS prioritises administrative efficiency over user needs, and lacks inclusive design, adaptive interfaces and secure communication mechanisms. The fragmentation of subsystems forces users to adjust to the technical architecture rather than the system adjusting to their needs. With respect to establishing conditions for cross-border judicial cooperation, interoperability, machine-readability, and data-driven justice, the findings indicate the necessity of implementing structured machine-readable data (XML/JSON) in judicial decisions, ECLI, and open APIs. The legislative enshrinement of these standards is not merely a requirement of «data-driven justice», but a mandatory legal prerequisite for the full deployment and use of the e-CODEX system in Ukraine. This is the only path to cross-border interoperability, which is critical for an EU candidate state. The implementation of these provisions requires amendments to Ukraine's procedural legislation (Commercial Procedural Code, Civil Procedural Code, Criminal Procedural Code, Code of Administrative Procedure, Code on Bankruptcy Procedures) or the adoption of a dedicated law, rather than reliance solely on technical concepts. The absence of these structural elements not only slows the reform but restricts the development of the LegalTech market and academic legal analytics, constituting a direct breach of the principle of data-driven justice.

The regulation of AI, to which increasing significance is attached in the Ukrainian justice system, is not characterised by a conceptual approach. Even at the level of the UJITS Concept, there is no requirement for mandatory assessment of the impact of AI systems on fundamental rights (in particular, in accordance with the requirements of the EU AI Act 2024/1689), nor is the establishment of an independent supervisory authority with effective powers to conduct independent supervisory audits and compliance assessments of AI systems used in judicial proceedings envisaged.

RECOMMENDATIONS

For the purpose of ensuring compliance with EU standards in the further digitalisation of the justice system in Ukraine, it is necessary to: ensure the systematic implementation of the principles of human-centred digital justice; coordinate digitalisation policies among judicial, law-enforcement and administrative bodies; and introduce monitoring of the compliance of national IT systems with the standards of human-centredness, inclusiveness and cross-border interoperability, to be carried out by a dedicated body. It is also required to introduce open APIs as a public service in the implementation of data-driven justice; establish mandatory accessibility requirements for digital judicial services in line with European standards; introduce the compulsory assignment of ECLI identifiers to all judicial decisions as a precondition for their legal validity; and legislate the status of AI exclusively as an assistive tool (following the classification of high-risk systems in the EU AI Act 2024/1689), with mandatory fundamental-rights impact assessment and human oversight at all stages of judicial decision-making.

Effective implementation of European standards of human-centred digital justice requires Ukraine not merely to modernise its technical infrastructure, but to undertake a fundamental shift in the governance and development paradigm of its justice system. This transition must be directed from a predominantly technological and managerial model towards a human-centred legal ecosystem, in which digital tools are subordinated to the unconditional protection of fundamental rights, the provision of inclusive access to justice, and the strengthening of public trust in the judiciary. Such an approach constitutes the pathway to the meaningful and successful integration of the national justice system into the European digital legal space and to the effective harmonisation with the EU acquis.

REFERENCES

[1] 2030 Digital Compass: the European way for the Digital Decade: European Commission, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: COM(2021) 118 final, 9 March 2021. Eur-lex. Access to European Union Law. Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52021DC0118.

[2] A European strategy for data: European Commission, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: COM (2020) 66 final, 19 February 2020. Eur-lex. Access to European Union Law. Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020DC0066.

[3] 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). PE/49/2023/REV/1. Eur-lex. Access to European Union Law. Retrieved from https://eur-lex.europa.eu/eli/reg/2023/2854/oj.

[4] A Digital Single Market Strategy for Europe: European Commission, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, COM(2015) 192 final, Brussels, 6 May 2015. Retrieved from https://ec.europa.eu/commission/presscorner/api/files/attachment/8210/DSM_communication.pdf.

[5] 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 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). PE/24/2024/REV/1. Retrieved from http://data.europa.eu/eli/reg/2024/1689/oj.

[6] Piatyhora, K. V. (2023). E justice in administrative process: European standards and foreign experience. Theory and Practice of Jurisprudence, 2(24), 39–57.

[7] 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 (General Data Protection Regulation). Eur-lex. Access to European Union Law. Retrieved from https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng.

[8] Directive (EU) 2016/680 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 by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA. Eur-lex. Access to European Union Law. Retrieved from https://eur-lex.europa.eu/eli/dir/2016/680/oj/eng.

[9] Ethics Guidelines for Trustworthy AI (2019, April). European Commission. Retrieved from https://op.europa.eu/en/publication-detail/-/publication/d3988569-0434-11ea-8c1f-01aa75ed71a1.

[10] Hyliaka, O. S. (2023). The latest technologies and human rights: an analysis of some critical issues of the digital era. *Journal of the National Academy of Legal Sciences of Ukraine*, 30(2), 15–30. [in Ukrainian]

[11] Burdin, M. Y., Nevzorov, I. L., & Najafli, E. (2024). European Experience of Digitalisation of the Executive Branch: Relevant Lessons for Ukraine. *Journal of the National Academy of Legal Sciences of Ukraine*, 31(1), 103–125. [in Ukrainian]

[12] Politanskyi, V. S. (2024). Experience in the Implementation and Operation of Electronic Justice Systems in European Countries. *Journal of the National Academy of Legal Sciences of Ukraine*, 31(3), 15–37. [in Ukrainian]

[13] Hyliaka, O. S. (2023). Right to privacy and protection personal data in digitalization conditions. *Journal of the National Academy of Legal Sciences of Ukraine*, 30(1), 15–30. [in Ukrainian]

[14] Sopilnyk, L. I., & Mykytiuk, M. A. (2023). European standards in information and legal support of e-government. *Academic Visions*, 16, 1–7. [in Ukrainian]

[15] Bernaziuk, O. O. (2021). Digital technologies in law: trends and prospects of development: PhD thesis abstract. Uzhhorod. [in Ukrainian]
[16] Nykon, O. Z. (2025). Digitalization of the justice system in Ukraine: theoretical and legal foundations: PhD thesis. Lviv: Lviv State University of Internal Affairs. Retrieved from https://www.lvduvs.edu.ua/documents_pdf/nauka/dorobok_zdobuvachiv/nicon_d.pdf. [in Ukrainian]
[17] Bohatchuk, D. (2025). Prospects for the development of electronic justice in Ukraine. Scientific Notes of NaUKMA. *Legal Sciences*, 15, 19–44. https://doi.org/10.18523/2617–2607.2025.15.19–44. [in Ukrainian]
[18] Bocharova, N. V. (2023). Human rights content of the digital transformation of the European Union. *Bulletin of Alfred Nobel University. Series «Law»,* 2(7), 41–49. Retrieved from https://law.duan.edu.ua/images/PDF/2023/2/5.pdf. [in Ukrainian]
[19] European Declaration on Digital Rights and Principles for the Digital Decade: The European Parliament, the Council and the Commission (2023). 2023/C 23/01. PUB/2023/89. Eur-lex. Access to European Union Law. Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=oj:JOC_2023_023_R_0001.
[20] Charter of Fundamental Rights of the European Union (2012). 2012/C 326/02. *European Parliament*. Retrieved from https://www.europarl.europa.eu/charter/pdf/text_en.pdf.
[21] Engel, A., & Groussot, X. (2025). Making the Rule of Law Great Again: The Building of the Digital Rule of Law in the European Union. In A. Engel, X. Groussot, & G. T. Petursson (Eds.), New Directions in Digitalisation. European Union and its Neighbours in a Globalized World, vol 13. Springer, Cham.
[22] Convention on the Rights of Persons with Disabilities (2006, December). Retrieved from https://zakon.rada.gov.ua/laws/show/995_g71#Text. [in Ukrainian]
[23] International Principles and Guidelines on Access to Justice for Persons with Disabilities (2020, August). United Nations. Geneva. Retrieved from https://www.un.org/development/desa/disabilities/wp-content/uploads/sites/15/2020/10/Access-to-Justice-EN.pdf.
[24] Union of Equality: Strategy for the Rights of Persons with Disabilities 2021–2030: European Commission, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions COM(2021) 101 final. *Eur-lex. Access to European Union Law.* Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021DC0101.
[25] A Union of Equality: Gender Equality Strategy 2020–2025: European Commission, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, COM(2020) 152 final, 5 March 2020. *Eur-lex. Access to European Union Law.* Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52020DC0152.
[26] Kremens, K., & Peristeridou, C. (2025). Everything, Everywhere All At Once: Virtual Criminal Justice in Europe. European Journal of Crime, Criminal Law and Criminal Justice, 33(1-2), 1–15. https://doi.org/10.1163/15718174–20250005.
[27] Onţanu, E. A. (2024). E-Justice governance in the EU. Contributions to Political Science. Strategies, Tools, and Implementation. Springer Cham, 243–258. https://doi.org/10.1007/978-3-031-56045-3_16.
[28] Depasquale, F. (2025). What will justice in the European Union look like in 10 years, and how could the legal professions in the EU innovate together? ERA Forum, 26, 41–50. https://doi.org/10.1007/s12027-025-00825-z.

[29] Syniehubov, O. V., Bortnik, O. H., & Chernenko, O. M. (2024). Ensuring the best interests of the child in the digital environment: European standards and national implementation challenges. *Juridical scientific and electronic journal*, 12, 137–143. https://doi.org/10.32782/2524–0374/2024–12/30. [in Ukrainian]

[30] The European Green Deal: European Commission, Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions, COM(2019) 640 final, 11 December 2019. *Eur-lex. Access to European Union Law*. Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52019DC0640.

[31] Sustainable Development Goals. *United Nations. Department of Economic and Social Affairs Sustainable Development.* Retrieved from https://sdgs.un.org/goals.

[32] European e-Justice Strategy 2024–2028 (2025, January). C/2025/437. Council of the European Union. *Eur-lex. Access to European Union Law.* Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52025XG00437.

[33] Kolesnikov, A. (2023). Legal Framework for Electronic Justice in the EU. Legal, Economic Science and Praxis. *Journal of Law and Social Sciences*, 8, 9–13. Retrieved from https://lesp.hu/wp-content/uploads/2024/08/2-Andrii-Kolesnikov_8_2023_p-9–13.pdf.

[34] Association Agreement between Ukraine, of the one part, and the European Union, the European Atomic Energy Community and their Member States, of the other part (2014, June). Retrieved from https://zakon.rada.gov.ua/laws/show/984_011#Text. [in Ukrainian]

[35] Report on the Initial Assessment of the Progress in the Implementation of the European Union Legal Acts (EU acquis) (2023, December). *Cabinet of Ministers of Ukraine*. Retrieved from https://eu-ua.kmu.gov.ua/wp-content/uploads/Zvit_EN.pdf?utm_source=chatgpt.com. [in Ukrainian]

[36] Maika, M. (2022). The Implementation of E-justice within the Framework of the Right to a Fair Trial in Ukraine: Problems and Prospects. Access to Justice in Eastern Europe, 3(15), 249–262. https://doi.org/10.33327/AJEE-18–5.2-n000320.

[37] Roadmap on the rule of law. *Office of the Deputy Prime Minister for European and Euro-Atlantic Integration.* Retrieved from https://eu-ua.kmu.gov.ua/wpcontent/uploads/UA_Dorozhnya_karta_z_pytan_verhovenstva_prava_2.pdf [in Ukrainian]

[38] How much will the new UJICS cost – the State Judicial Administration announced the cost of the project calculated until 2029 (2025, October). *Judicial and Legal Gazette.* Retrieved from https://sud.ua/uk/news/publication/342680-skolko-budet-stoit-novaya-esiks-v-gsa-soobschili-o-stoimosti-proekta-rasschitannogo-do-2029-goda. [in Ukrainian]

[39] Regulation on the procedure for the functioning of individual subsystems (modules) of the Unified Judicial Information and Telecommunication System (UJITS): Decision of the High Council of Justice (2021, August). Retrieved from https://zakon.rada.gov.ua/rada/show/v2623910-24#Text. [in Ukrainian]

[40] On approval of the UJITS Concept: State Judicial Administration of Ukraine (2025, April). Retrieved from https://court.gov.ua/storage/portal/dsa/news/Kontseptsia%20ESIKS.pdf. [in Ukrainian]

[41] eCourt mobile application (Google Play Store). Retrieved from https://play.google.com/store/apps/details?id=com.floor12apps.ecourt&hl=uk. [in Ukrainian]

[42] On approval of the Concept for the development of artificial intelligence in Ukraine: Order of the Cabinet of Ministers of Ukraine (2020, December). Retrieved from https://zakon.rada.gov.ua/laws/show/1556–2020-%D1%80#n8. [in Ukrainian]

[43] On approval of the action plan for the implementation of the Concept for the development of artificial intelligence in Ukraine for 2025–2026: Order of the Cabinet of Ministers of Ukraine (2025, May). Retrieved from https://zakon.rada.gov.ua/laws/show/457–2025-%D1%80#Text. [in Ukrainian]
[44] On approval of the Code of Judicial Ethics: Congress of Judges of Ukraine (2024, September). Retrieved from https://zakon.rada.gov.ua/rada/show/n0001415-24#Text. [in Ukrainian]
[45] The Commercial Procedural Code of Ukraine (1991, November). Retrieved from https://zakon.rada.gov.ua/laws/show/1798–12#Text. [in Ukrainian]
[46] The Criminal Procedural Code of Ukraine (2012, April). Retrieved from https://zakon.rada.gov.ua/laws/show/4651–17#Text. [in Ukrainian]
[47] The Civil Procedural Code of Ukraine (2004, March). Retrieved from https://zakon.rada.gov.ua/laws/show/1618–15#Text. [in Ukrainian]

Олег Васильович Синєгубов
Доктор юридичних наук, професор
Член-кореспондент НАПрН України
Національна академія правових наук України
61024, вул. Григорія Сковорода, 70, Харків, Україна

Голова Харківської обласної військової адміністрації
61002, вул. Сумська, 64, Харків, Україна

Oleg V. Sinegubov
Doctor of Law Sciences, Professor
Corresponding Member NALS of Ukraine
National Academy of Legal Sciences of Ukraine
61024, 70 Hryhoriia Skovorody St., Kharkiv, Ukraine

Head of Kharkiv Regional Military Administration
61002, 64 Sumskaya St., Kharkiv, Ukraine

Email: sinegubov.oleg@gmail.com
ORCID: https://orcid.org/0000-0001-6362-3115

Оксана Григорівна Бортнік
Кандидат юридичних наук, доцент
Доцент кафедри цивільного, трудового та господарського права
Харківський національний університету внутрішніх справ
61000, проспект Льва Ландау, 27, Харків, Україна

Oksana G. Bortnik
Candidate of Law Sciences, Associate Professor
Associate Professor at the Department of Civil, Labour and Commercial Law
Kharkiv National University of Internal Affairs
61000, 27 Lev Landau Ave., Kharkiv, Ukraine

Email: bortnikoksana1980@gmail.com
ORCID: https://orcid.org/0000-0001-7816-0387

Олена Михайлівна Черненко
Кандидат юридичних наук
Доцент кафедри публічного управління, адміністрування та права
Національний університет «Полтавська політехніка імені Юрія Кондратюка»
36000, проспект Віталія Грицаєнка, 24, Полтава, Україна

Доцент кафедри права
Приватний вищий навчальний заклад «Європейський університет»
03115, бульвар Академіка Вернадського, 16В, Київ, Україна

Olena M. Chernenko
Candidate of Law Sciences
Associate Professor at the Department of Public Management, Administration and Law
National University «Yuri Kondratyuk Poltava Polytechnic»
36000, 24 Vitalii Hrytsaienko Ave., Poltava, Ukraine

Associate Professor at the Department of Law
Private Higher Educational Institution «European University»
03115, 16V Academician Vernadsky Blvd., Kyiv, Ukraine

Email: olena.chernenko22@gmail.com
ORCID: https://orcid.org/0000-0003-4178-5417

Suggested Citation: Sinegubov, O. V., Bortnik, O. G., & Chernenko, O. M. (2025). Principles of Human-Centred Digital Justice: the European Approach and Ways of Implementation in Ukraine. *Journal of the National Academy of Legal Sciences of Ukraine,* 32(4), 84–111.

Стаття надійшла / Submitted: 03/11/2025
Доопрацьовано / Revised: 03/12/2025
Схвалено до друку / Accepted: 18/12/2025