4. CONTRACTUAL AND OTHER LEGAL RELATIONS IN THE DIGITAL ENVIRONMENT

UDC: 347.44:004
DOI: 10.5937/PDSC26022M

Predrag Mirković, PhD, Full Professor
Faculty of Law for Commerce and Judiciary in Novi Sad,
University Business Academy in Novi Sad
ORCID ID: https://orcid.org/0000-0003-2323-040X,
email: mirkovic@pravni-fakultet.info

DIGITAL IDENTITY AND DIGITAL CONTRACTING: AUTHENTICATION, LEGAL CERTAINTY AND THE FULFILMENT OF CONTRACTUAL OBLIGATIONS

Abstract: The development of contemporary digital society and the digital economy has changed not only how contractual relations are formed, but also how legally relevant conduct is identified, evidenced and attributed in the digital environment. This is particularly visible in digital contracting, where contractual communication often takes place without the physical presence of the parties and depends on digital data, electronic identification mechanisms and trust services. In these circumstances, digital identity cannot be reduced to a purely technical question of access to a system or platform.This paper examines the legal role of digital identity in digital contracting, especially in relation to the formation of contractual relations, confirmation of the parties' identity, expression of contractual will and fulfilment of contractual obligations. The aim of the paper is to determine the significance of digital identity for authentication, legal certainty and trust in digital contractual relations. Particular attention is given to offer and acceptance of one in electronic form, proof of contractual will, electronic identification, legal attribution of digital actions and the legal effects of trust services. The paper also considers the limits of electronic contracting, especially in cases where stricter legal forms are required. The research in this paper concludes that digital identity has moved beyond its initial technical function and it has become a legally relevant concept of digital

society, particularly in digital contracting, but also a digital identity does not replace traditional institutes of contract law bud rather it enables their application in circumstances in which contractual will, contractual obligation and contractual performance are expressed through digital means.

Keywords: *digital identity, digital contracting, authentication, legal attribution, electronic identification.*

1. INTRODUCTORY REMARKS

The development of contemporary digital society and the digital economy has changed the way legal relations are created, conducted and fulfilled. Digital technology is no longer merely a means of communication between legal subjects. It is increasingly becoming the environment in which legal relations are formed, confirmed and performed. This change is particularly visible in contract law, where traditional models of contracting are being supplemented, and in some situations replaced, by digital forms of communication and electronic commerce. In traditional contracting, the identity of the contracting parties can usually be established directly or through relatively stable legal mechanisms: identity documents, signatures, powers of attorney, registration data or other forms of individualisation of the legal subject. Digital contracting is different. The parties do not have to be physically present, and their communication takes place through digital data, electronic identification, authentication, user accounts, electronic signatures and trust services. For that reason, identity acquires particular legal significance in digital contracting.But, it is not enough to establish that a particular digital action has technically been performed. From the perspective of contract law, the more important question is whether that action can be attributed to a particular legal subject. In other words, it must be possible to know who made the offer, who accepted it, who expressed contractual will and who assumed a particular contractual obligation. If this connection cannot be reliably established, the legal certainty of digital contracting becomes questionable. In this context, digital identity should not be understood only as a technical mechanism for accessing a digital service or electronic platform. It increasingly appears as a legally relevant concept that enables a digital action to be linked to a particular legal subject.

The subject of this paper is the analysis of digital identity in the context of digital contracting, with particular emphasis on its importance for the authentication of contracting parties, the legal certainty of electronic transactions, the legal attribution of digital actions and the fulfilment of

contractual obligations. The aim of the paper is to determine whether digital identity has only a technical function of identifying participants in a digital transaction, or whether it also acquires broader significance for contract law. In other words, the paper seeks to show that the legal relevance of digital identity does not arise from technology itself, but from the possibility of linking a specific digital action to a particular legal subject and recognising that action as capable of producing contractual legal effects. The main hypothesis of the paper is that, in digital contracting, digital identity does not merely confirm the identity of participants, but also performs the function of legally attributing a digital declaration of will, contractual obligation and act of fulfilment to a particular legal subject. Such a function does not abolish the classical institutes of the law of obligation but rather, it enables their application in a digital environment, where declarations of will, evidentiary processes and fulfilment of obligations are increasingly carried out through electronic means.

This understanding builds on contemporary theoretical approaches that treat digital identity as a legal concept, not merely as a technical set of digital data (Sullivan, 2011; Robles-Carrillo, 2024; Stojšić Dabetić, Mirković, & Aleksić Oliveira, 2025). On that basis, the paper seeks to show that digital identity is not an institute that replaces traditional institutes of the law of obligations. Its function is different. It allows the rules on offer, acceptance, agreement of wills, fulfilment of obligations and liability to be applied in a changed technological environment. In that sense, digital identity is a legally relevant category that gives traditional rules of contract law a new functional dimension in digital legal transactions.

2. Digital identity as a legal concept of digital society

Every legal relationship presupposes the existence of a subject to whom certain rights, obligations, powers or responsibilities are attached. For that reason, identity is not only a matter of personal, social or technical recognition. It is one of the fundamental questions of the legal order. Law must be able to identify the subject of a legally relevant act, because only then can it determine who acquires a right, who assumes an obligation, who expresses legally relevant will and who bears the consequences of a particular act. In traditional legal transactions, the identity of a legal subject is confirmed by various legally recognised means. For natural persons, these primarily include identity documents, handwritten signatures, physical presence or other forms of proving personal status. For legal persons, identity is established through registration data, business name, registered

seat, registration number and authority of representatives. These models of identification were developed in a legal environment in which most legal relations were based on direct communication or the use of physical documents.

The development of digital society has changed this model. An increasing number of legal relations are created, conducted and fulfilled in the digital environment, without direct contact between legal subjects. In such an environment, a subject does not act only through physical presence or a material document, but through digital data, user accounts, electronic signatures, certificates, platforms, applications and other technological mechanisms. In other words, a legal subject appears in the digital environment through a particular digital trace. The legal question is whether that trace can be reliably linked to the person who acquires rights or assumes obligations in legal transactions.

In legal literature, digital identity is increasingly viewed as a new legal concept rather than only as a technical set of data. Sullivan analyses digital identity in a transactional context and points out its particular relevance in legal and commercial relations conducted electronically (Sullivan, 2011). Robles-Carrillo emphasises that digital identity is not merely a digital version of physical identity, but a complex construct that provides the basis for access to the digital world and participation in different forms of digital transactions and communication (Robles-Carrillo, 2024). This approach is important because it shifts the discussion from the technical level to the legal level.

Digital identity may be understood as a set of digital data, identifiers, attributes and mechanisms through which a person is identified, authenticated and verified in a digital environment. Its legal meaning, however, is not exhausted by the fact that a person has a user account, password, email address or another form of digital representation. It becomes legally relevant only when it enables a particular digital action to be linked to a specific legal subject. This is the core legal issue. The decisive question is not only whether a digital record exists, but whether it makes it possible to determine who performed the action and to whom its consequences may be attributed. This understanding of digital identity is particularly important because, in contemporary digital society, a large part of legal and economic transactions takes place without direct contact between the participants. The digital economy and the information society create new models of communication, business and contracting, in which traditional legal institutes are applied in a changed technological environment (Dukić Mijatović & Mirković, 2022). In that context, digital

identity becomes one of the instruments through which the legal subject is recognised in the digital environment and through which that subject's action receives a legal qualification.

Digital identity must be distinguished from related concepts such as electronic identification, authentication and verification. The European normative framework confirms this direction of development. The eIDAS Regulation established a legal framework for electronic identification and trust services for electronic transactions in the internal market of the European Union. The later amendment of this regime through Regulation (EU) 2024/1183 further develops the European digital identity framework and confirms that digital identity is increasingly regarded as a regulatory precondition for secure participation of natural and legal persons in digital services and electronic transactions (European Parliament and Council, 2014; European Parliament and Council, 2024). In this way, digital identity moves beyond the narrow understanding of the electronic signature and acquires broader significance in digital legal transactions. Theoretical discussions on European digital identity also highlight the need to distinguish between digital identity, decentralised identity and the self-sovereign identity model. Biedermann, Scerri, Kozlova and Ellul (2024) point out that these concepts are often used imprecisely, although they have different technical and regulatory assumptions. This observation is important for legal analysis as well, because the legal significance of digital identity cannot be based merely on the general fact of digital representation, but on the legally regulated possibility of using a particular identity in legally relevant digital transactions. Similarly, Sitouah, Esposito and Bruschi (2026) analyse eIDAS 2.0 in relation to control, privacy and the legal implications of digital identity, confirming that the contemporary digital identity framework develops through a connection between technical architecture and legal effects.

In this respect, the distinction between general digital identity, transactional identity and registered digital identity is particularly significant. General digital identity may include different forms of a person's digital representation in the digital environment. Transactional identity refers to the identity used in a specific digital transaction, that is, in a particular legal or business relationship. Registered digital identity presupposes an identity that has been previously established, recorded and connected with a particular legal subject through an appropriate system of registration or electronic identification. This distinction matters because not every form of digital representation produces the same degree of legal certainty. A username and password may enable access to a platform, but

they do not necessarily have the same legal significance as a qualified electronic signature or another form of electronic identification based on a reliable identity verification system.

For that reason, digital identity cannot be seen as a complete replacement for the legal identity of a natural or legal person. A natural person remains a natural person, and a legal person retains its legal personality independently of the digital mode of representation. Digital identity, however, becomes the way in which that subject appears, is confirmed and acts in the digital environment. It has an intermediary function, because it connects traditional legal personality with the digital manner of performing legal acts. This connection between subject, action and consequence is the basis of the legal relevance of digital identity. This function is especially visible in digital contracting. In contracts, it is essential to establish who made the offer, who accepted it and who expressed contractual will. When a contract is concluded without direct contact between the parties, reliable identification of the participants becomes one of the basic prerequisites of legal certainty. Without the possibility of linking a digital declaration to a particular legal subject, it becomes disputed who participated in the contractual relationship, who assumed the obligation and against whom rights under the contract may be enforced.

3. Digital identity and digital contracting

A contract, as one of the fundamental institutes of the law of obligations, is based on the agreement of the parties' wills. For a contract to come into existence, there must be a legally relevant declaration of will by one party, most often expressed through an offer, and a corresponding declaration of will by the other party, expressed through acceptance. The existence of an offer and acceptance, however, presupposes that it is possible to determine who made the declaration of will, to whom it was addressed and who assumed a particular contractual obligation on its basis. For that reason, the identity of the contracting parties is not a secondary issue of contract law. It is directly connected with the legal certainty of the contractual relationship.

In traditional contracting, the identity of the parties is confirmed through physical presence, signature, public or private documents, powers of attorney, registration data or other legally recognised means of identification. Such mechanisms make it possible to connect a declaration of will with a particular legal subject. In digital contracting, the parties do not have to be physically present, and their communication does not have to be based on a physical document. Contractual will may be expressed by email,

an online platform, a user account, an electronic form, an electronic signature or another means of digital communication. The traditional question of agreement of wills is thereby transferred to the digital environment. Digital contracting does not change the basic structure of the contract, but it does change the circumstances in which the contract is concluded, confirmed and proved. Offer and acceptance remain the key elements of the contractual cycle, but their expression takes place in a different technological setting. Digital technology therefore does not abolish traditional rules of contract law. It requires those rules to be interpreted in light of new forms of communication and new ways of expressing contractual will. This is why the identity of the person participating in a digital transaction is particularly important in the analysis of digital contracting. This question is directly linked to the analysis of offer and acceptance in electronic contracts, since it is precisely in these phases of the contractual cycle that the question arises most clearly: who expressed contractual will and under what conditions can that expression be treated as legally relevant (Stojšić Dabetić & Mirković, 2024).

In this context, digital identity performs the function of linking a digital declaration of will to a specific legal subject. When a contract is concluded electronically, it is not enough to establish only that a particular digital action was technically performed. The legally decisive issue is whether that action can be attributed to a particular person, that is, whether it can be treated as an expression of the will of a specific contracting party. If that connection is not reliable, it may be disputed who made the offer, who accepted it, who assumed the contractual obligation and who bears responsibility for non-fulfilment. In that sense, digital identity is a legally relevant mechanism connecting the legal subject, the digital action and the legal consequence (Stojšić Dabetić, Mirković, & Aleksić Oliveira, 2025).

In digital contracting, it is necessary to distinguish between the technical performance of a digital action and its legal attribution to a contracting party. The fact that an action was performed through a user account, platform or electronic means of communication does not by itself mean that it can automatically be treated as a declaration of will by the person whose identity was used. For contract law, what matters is whether there is a sufficiently reliable connection between the digital action, the declaration of will and the legal subject to whom that declaration is attributed. In other words, digital contracting does not raise only the question of the form of the declaration of will but it also raises the question of trust in the identity of the person acting in electronic legal transactions. This approach is also supported by the UNCITRAL Model Law on Electronic Commerce,

especially by the rules on the attribution of electronic messages to their originator. The rules on attribution of data messages show that electronic communication does not merely produce a technical trace, but raises the question under what conditions that trace may be treated as the action of a particular subject. The United Nations Convention on the Use of Electronic Communications in International Contracts has a similar function, since it proceeds from the need to recognise the legal functionality of electronic communication in international contracts and to remove obstacles arising from its electronic form (United Nations, 2005). Gabriel (2006) notes that this Convention provides uniform standards for international contracting by electronic means, while Mik (2011) emphasises its importance in removing obstacles to the use of electronic communications in international contracts and in strengthening legal certainty and predictability.

From the perspective of domestic law of obligations, this issue should be considered in connection with the general rules on contract formation, offer and acceptance. The Law on Obligations proceeds from the rule that a contract is concluded when the parties agree on its essential elements. This rule, contained in Article 26, remains the starting point for digital contracting as well. The digital environment does not change the need for agreement of wills, but it changes the way in which that agreement is expressed and proved. The rules on offer and acceptance are particularly important in this respect. Article 38 of the Law on Obligations provides that an offer to conclude a contract for which the law requires a special form binds the offeror only if it is made in that form, and the same applies to acceptance. Article 39 of the same law provides that an offer is accepted when the offeror receives the offeree's statement of acceptance, but also when the offeree sends goods, pays the price or performs another act which, on the basis of the offer, established practice between the parties or custom, may be regarded as a statement of acceptance. These rules are especially relevant for digital contracting because they show that a declaration of will does not always have to be made in classical written form but may also be result from conduct that has the meaning of acceptance.

This is precisely where the basic problem of digital contracting arises. If acceptance is expressed by a click, confirmation of an electronic order, sending an electronic message or using an electronic signature, it must be established who performed that action. In other words, contract law does not require digital identity as a separate condition for the validity of a contract, but it does require the possibility of attributing the declaration of will to a particular contracting party. The problem is not whether the digital action existed, but whether that action can be legally attributed to the person bound

by the contract. For this reason, digital identity represents one element of legal certainty in digital contracting. Its role is not limited to the technical possibility of accessing an electronic platform or digital service. It enables the contractual act to be individualised and connected with a particular contracting party. In this way, it ensures a legally relevant connection between digital communication and the contractual legal consequence that follows from that communication. This approach is consistent with a broader understanding of contract law in digital society, according to which digitalisation does not bring an end to traditional contractual institutes, but requires their functional adaptation to a new technological environment (Stojšić Dabetić & Mirković, 2022).

The significance of digital identity is particularly evident at the stage of concluding an electronic contract. In electronic contracting, an offer may be made through a website, electronic platform, application or another form of electronic communication. Acceptance may be expressed by sending an electronic message, clicking the appropriate field, confirming an order, using an electronic signature or through other conduct that, in the given context, has the meaning of acceptance. However, for such conduct to have contractual legal significance, it must be established whether it was performed by a person who has legal capacity and authority to enter into the contractual relationship. Therefore, in electronic contracts, the issue of offer and acceptance cannot be separated from the identification of the contracting parties (Stojšić Dabetić & Mirković, 2024).

Digital identity is also connected with proof of contractual will. In the digital environment, contractual will is usually not expressed through a traditional handwritten signature on a physical document, but through an electronic trace. That trace may be an electronic message, a record of acceptance of terms of use, confirmation of an electronic order, a qualified electronic signature or another form of digital record. However, the legal value of such a trace depends on the possibility of linking it to a particular legal subject. Digital identity, electronic identification and trust services therefore have significance not only for the technical security of a transaction, but also for proving the existence of contractual will. In the European legal framework, these issues are normatively linked to electronic identification and trust services for electronic transactions, confirming that the reliability of digital identification is viewed as an important element of legal certainty in electronic commerce (European Parliament and Council, 2014).

The domestic legal framework recognises the possibility of concluding contracts in electronic form. Article 9 of the Law on Electronic Commerce

expressly provides that a contract may be concluded electronically, that is, in electronic form, and that an offer and acceptance may also be made electronically, that is, in electronic form. The same article provides that a contract may not be denied validity solely because it was made in electronic form. Electronic form is thereby recognised as a legally relevant form of contracting. However, this rule does not in itself resolve the identity of the person who made the electronic declaration of will. It only confirms that electronic form is not a ground for contesting the contract, while the attribution of the declaration of will remains a matter of identification, authentication and proof.

The rule on the validity of electronic contracts is not unlimited. Article 10 of the Law on Electronic Commerce provides for exceptions to the application of the rules on electronic contracting, particularly in relation to contracts which, under a special law, may not be concluded in electronic form, and in relation to contracts and other legal transactions for which the form of a publicly certified document, notarial deed or certified signature is prescribed, unless otherwise provided by a special law or by regulations governing signature certification, certification and drafting of documents. This limitation is important because it shows that digital contracting does not abolish requirements of form, but must respect them to the extent that they are prescribed for particular legal transactions. A similar logic exists in international models of electronic commerce. The UNCITRAL Model Law on Electronic Commerce proceeds from the need to recognise the legal functionality of electronic means of communication in commercial transactions. Its basic idea is not to create an entirely new contract law, but to remove obstacles that would arise from the fact that a particular communication or declaration is made in electronic form. This approach corresponds to a functional understanding of digital contracting: legal significance does not depend solely on the form in which the declaration is made, but on whether its content, originator, addressee and legal effect can be established (UNCITRAL, 1996).

On this basis, digital identity has at least three legally relevant functions in digital contracting. The first is an identification function, because it enables the subject participating in the contractual relationship to be identified. The second is an evidentiary function, because it enables a digital declaration of will to be linked to a particular person. The third is a legal certainty function, because it enables the contractual obligation to be attached to a specific legal subject and, in the event of a dispute, enables responsibility for its fulfilment or non-fulfilment to be established. Digital identity, therefore, does not introduce a new logic into the law of

obligations. It enables existing rules on offer, acceptance and agreement of wills to be applied in the digital environment. Its function in contract law is not to replace the rules of the Law on Obligations, but to secure the link between electronically expressed will and a specific legal subject.

4. Normative framework of electronic identification and trust services – the question of authentication

Digital identity, as a legally relevant concept of digital society, cannot be viewed separately from the normative framework governing electronic identification, electronic documents and trust services. If digital identity is to enable the linking of a legal subject with a digital action and a legal consequence, there must be rules determining the manner of confirming identity, the reliability of electronic communication and the legal effect of electronic actions. In traditional legal transactions, trust in the identity of a legal subject is secured through various legally recognised mechanisms, such as identity documents, registers, handwritten signatures, seals, powers of attorney or certification of a particular document. In the digital environment, these mechanisms acquire their functional equivalents. Electronic documents, electronic signatures, electronic identification, electronic seals, electronic time stamps, electronic delivery and other trust services are intended to enable legally secure communication and reliable linking of a digital action to a particular legal subject.

The law of the Republic of Serbia recognises the significance of these issues through the Law on Electronic Documents, Electronic Identification and Trust Services in Electronic Business. This law regulates electronic documents, electronic identification and trust services in electronic business, thereby recognising electronic business as a legally relevant form of action by natural and legal persons in the digital environment (Law on Electronic Documents, Electronic Identification and Trust Services in Electronic Business, 2017/2021). Such a normative definition shows that electronic business is not treated merely as a technical form of communication, but as a legally significant form of conduct in contemporary legal transactions. The normative framework of electronic identification and trust services should be viewed in functional connection with the rules of contract law. The Law on Electronic Documents, Electronic Identification and Trust Services in Electronic Business does not regulate the contract as an institute of the law of obligations, but it provides instruments that make an electronic action legally more reliable. This is particularly visible in the case of electronic signatures, electronic seals and electronic time stamps.

Article 50 of this law provides that an electronic signature may not be denied validity or evidentiary force solely because it is in electronic form or because it does not meet the conditions for a qualified electronic signature. At the same time, a qualified electronic signature has the same legal effect as a handwritten signature. This rule is particularly important for digital contracting because it shows that the electronic form of a signature is not a legal obstacle, but that different forms of electronic signature do not always have the same evidentiary value. The electronic seal has a similar function. Article 51 of the same law provides that an electronic seal may not be denied validity or evidentiary force solely because it is in electronic form, while a qualified electronic seal carries a legal presumption of data integrity and accuracy of origin for the data to which it is linked. In a contractual context, this is especially important for legal persons, because an electronic seal may help prove the origin of an electronic document and its connection with a particular legal subject.

Article 53 of the same law regulates the legal effect of an electronic time stamp, providing that it may not be denied validity or evidentiary force solely because it is in electronic form or because it does not meet the conditions for a qualified time stamp. This normatively recognises the importance of the time at which an electronic action is performed. In digital contracting, this may be decisive for determining when an offer was made, when acceptance was sent or received, and whether a particular obligation was fulfilled on time.

The contractual significance of this framework is further confirmed by the Law on Electronic Commerce. This law defines a contract in electronic form as a contract concluded between an information society service provider and a service user electronically, through the use of electronic means (Law on Electronic Commerce, 2009/2013/2019). In this way, electronic contracting is recognised as a legally relevant manner of creating a contractual relationship. However, recognition of the electronic form of a contract is only the first step. For an electronic contract to be legally secure, reliable identification of the parties, confirmation of their contractual will and proof of the actions performed in the digital environment must also be ensured. For this reason, the Law on Electronic Commerce and the Law on Electronic Documents, Electronic Identification and Trust Services must be viewed as interconnected parts of the normative framework of digital contracting. The first law regulates the conditions and legal significance of electronic commerce and electronic contracts, while the second provides legal instruments that make electronic communication, identification and documentation more reliable. Together, these rules enable traditional

institutes of contract law to be applied in the digital environment, while taking into account the specific features of electronic communication, electronic form and digital identity.

The European legal framework is particularly important for understanding the development of digital identity. The 2014 eIDAS Regulation established a legal framework for electronic identification and trust services for electronic transactions in the internal market of the European Union (European Parliament and Council, 2014). Its basic function was to ensure legal recognition and mutual trust in electronic identification and trust services in cross-border digital business. It thus laid the normative foundation at EU level for reliable participation of natural and legal persons in electronic transactions. The eIDAS Regulation contains a similar logic. Article 25 provides that an electronic signature may not be denied legal effect or admissibility as evidence solely because it is in electronic form or because it does not meet the requirements for a qualified electronic signature, while a qualified electronic signature has the equivalent legal effect of a handwritten signature. Article 26 sets out the requirements for an advanced electronic signature, including that it must be uniquely linked to the signatory, capable of identifying the signatory, created using signature creation data under the signatory's control, and linked to the signed data in such a way that any subsequent change is detectable. Article 35 regulates the legal effect of an electronic seal and the presumption of data integrity and accuracy of origin in the case of a qualified electronic seal.

The development of digital society has shown, however, that electronic identification and electronic signatures are not sufficient for all increasingly complex forms of digital legal transactions. Regulation (EU) 2024/1183 therefore established the European Digital Identity Framework, amending the previous eIDAS regime (European Parliament and Council, 2024). This Regulation confirms that digital identity is no longer viewed only as electronic identification in a narrow sense, but as a broader regulatory concept intended to enable safer, interoperable and reliable participation of subjects in digital services. The concept of the European Digital Identity Wallet is particularly important within the new European framework. Its legal relevance for digital contracting is not limited to the technical storage of identification data. It lies in the possibility for a user to use verifiable identity data and other attributes in digital transactions, where those attributes may be relevant for the conclusion and fulfilment of a contract. In contractual relations, such a mechanism may contribute to a more reliable

transactional identity, particularly where it is necessary to confirm identity, authority to represent or other relevant attributes of a contracting party.

The normative framework, however, does not remove all legal dilemmas. Questions remain regarding the different levels of reliability of digital identity, the relationship between technical authentication and legal identification, and the legal consequences of misuse of digital identity. It is particularly important to distinguish between situations in which a contract is concluded by simple use of a user account and password and situations in which a qualified electronic signature or another qualified trust service is used. Both forms may have practical importance in digital business, but their evidentiary and legal reach is not the same. These rules show that the normative framework does not create digital identity as a social or technological fact, but gives it a legal function. It determines when electronic signatures, seals, time stamps and other trust services may have evidentiary value, legal effect and significance for linking a digital action to a particular subject. This is where their connection with contract law is found: a contract is formed and fulfilled under the rules of the law of obligations, but digital identity and trust services help establish who performed the action, when it was performed and whether it can be legally attributed to a contracting party.

It follows that digital identity acquires its full legal significance only in connection with normative rules governing electronic identification, electronic documents and trust services. Without such rules, digital identity could remain primarily a technical or platform-based category. Once normatively recognised, it becomes part of the legal infrastructure of digital society. In this sense, the domestic, European and international legal framework confirms that digital identity is one of the key prerequisites of legal certainty in digital legal transactions, particularly in digital contracting.

5. Digital identity as a prerequisite of legal certainty in digital transactions

In digital contracting, it is not enough to prove only that an electronic message was sent, that a user accessed a platform or that a particular action was technically recorded. In a dispute, it will be necessary to determine the origin of the message, the time of sending and receipt, the accessibility of the message to the recipient, the reliability of the identification mechanism and the connection between the electronic action and the contracting party. This is precisely where digital identity shows that it is not merely a technical

precondition for digital communication, but one of the elements of legal certainty in digital legal transactions.

Digital identity in digital transactions has at least two dimensions. The first is technical, because it enables access to a system, platform or digital service. The second is legal, because it enables a digital action to be linked to a particular subject and, under certain conditions, recognised as producing contractual legal effects. These two dimensions should not be equated. Technical access to a system may be an indicator of identity, but it is not always a sufficient basis for concluding that a legally relevant declaration of will exists.

The legal certainty of digital transactions depends on the reliability of the identification mechanism. A simple user account, email address or password may be sufficient for everyday low-risk transactions, but it may not be sufficient for more complex contractual relations. By contrast, a qualified electronic signature, electronic seal, electronic time stamp and other trust services have greater evidentiary significance because they are based on normatively regulated and technically more reliable mechanisms for confirming identity, origin and integrity of an electronic action. Legal certainty in digital transactions is particularly connected with proof of contractual will. In digital contracting, the declaration of will is usually not expressed in a traditional written document with a handwritten signature, but through an electronic trace: a click, electronic message, order confirmation, digitally signed document or another form of electronic communication. Such a trace may be evidentially relevant, but its legal value depends on whether it can be linked to a particular legal subject and whether, in light of the circumstances of the case, it may be treated as an expression of that subject's contractual will. In this context, the rules on confirmation of receipt and the time of conclusion of an electronic contract are particularly important. Article 14 of the Law on Electronic Commerce provides that the service provider must, without delay, confirm receipt of an electronic message containing an offer or acceptance for the conclusion of a contract by electronic means and through a separate electronic message. Article 15 of the same law provides that a contract in electronic form is deemed concluded when the offeror receives the electronic message containing the offeree's statement of acceptance, while an offer, acceptance and other electronic declarations of will are deemed received when the addressee is able to access them.

These rules are important because they show that digital contracting is not exhausted by the question whether electronic form has legal effect. It is equally important when the electronic declaration was sent, when it was

received and whether the subject from whom it originates can be established. In this sense, the time of receipt of an electronic declaration and the identity of its sender are connected questions. A contract may be regarded as concluded only when the requirements relating to the content of the declaration, its receipt and the possibility of attributing it to a particular contracting party are satisfied.

Similar issues in the international context are addressed by the United Nations Convention on the Use of Electronic Communications in International Contracts. Its rules are aimed at removing obstacles to the use of electronic communications in international contracting and at recognising electronic communications as legally relevant equivalents of traditional forms of communication (United Nations, 2005). Gabriel (2006) views this instrument as an attempt to establish uniform standards for international electronic contracting, while Mik (2011) points out that its value lies not only in the recognition of electronic form, but also in strengthening legal certainty and commercial predictability. These sources confirm that legal certainty in digital transactions depends on addressing three questions at the same time: whether the electronic declaration is legally recognised, when it produces effect and to whom it may be attributed.

Digital identity also has an important evidentiary function in the event of a dispute. If one contracting party denies having concluded the contract, accepted the offer, placed an order or agreed to certain terms, the decisive issue will not be the mere existence of an electronic record. It will be necessary to determine whether that record originates from a particular contracting party, whether it was created in circumstances indicating the existence of contractual will and whether the other party could reasonably rely on that form of conduct. Also, the misuse of digital identity is a particularly significant problem in digital environment. One person may use another person's account, misuse a password, access an electronic service without authorisation or present themselves as another person. In such situations, it would be wrong to conclude mechanically that every action performed through a particular account binds the person to whom the account relates. It must be examined whether the person whose identity was used acted with due care, whether the other contracting party had grounds to rely on the digital identity, whether the identification system was sufficiently reliable and whether there are circumstances indicating unauthorised use of identification data. In cases of misuse of digital identity, the issue of legal certainty is directly connected with the allocation of risk. The risk cannot always automatically be borne by the person whose account was used, but neither can it always be shifted to the other contracting party

that relied on the available identification data. The answer depends on the nature of the contract, the reliability of the identification means, the conduct of the parties, the contractual rules on account use and the general rules on good faith, due care and liability.

Trust services are designed to reduce these risks, but not to eliminate them completely. Electronic signatures, electronic seals, time stamps and electronic delivery may increase the evidentiary reliability of a digital action. Nevertheless, they do not remove the need for legal assessment in the specific case. The legal significance of these mechanisms does not lie in the idea that technology itself produces legal certainty, but in the fact that the legal order recognises certain electronic means as having evidentiary and legal functions.

It follows that digital identity has four functions in relation to the legal certainty of digital transactions. The first is identification, because it enables the person participating in the transaction to be determined. The second is authentication, because it confirms that the person acts through a particular identification mechanism. The third is evidentiary, because it enables a digital action to be linked to a particular legal subject. The fourth is responsibility-related, because it enables the legal consequences of a digital action, under conditions recognised by law, to be attached to a particular contracting party. Accordingly, legal certainty in digital transactions does not depend only on the recognition of the electronic form of a contract. It also depends on whether it can be established who made the declaration, when it was received, whether the other party could reasonably rely on the digital identity and whether the consequences of the specific digital action can be legally attributed to a particular subject. Only in this connection does digital identity acquire its full significance for contract law.

6. Digital identity and the fulfilment of contractual obligations in the digital environment

In traditional law of obligations, fulfilment of obligations is linked to the relationship between parties. For example, the debtor is the person obliged to perform a particular act, while the creditor is the person entitled to require its performance. Such a relationship presupposes that the subjects of the obligation are known and legally individualised. If it cannot be established who the debtor or creditor is, it becomes difficult to determine the content of the obligation, its maturity, the manner of fulfilment and liability for breach of contract. For that reason, the identity of the contracting parties is

important not only for the creation of the contract, but also for its performance.

From the perspective of the Law on Obligations, fulfilment remains the central stage of the obligation relationship, because the contract achieves its legal and economic purpose only when the obligations assumed are performed. Article 296 of this law provides that an obligation may be fulfilled not only by the debtor, but also by a third party, while the creditor is obliged to accept fulfilment from a person who has a legal interest in the obligation being fulfilled, and even from a third party if the debtor agrees, unless under the contract or the nature of the obligation the performance must be carried out personally by the debtor. This rule is important in the digital environment because it shows that the identity of the person performing an obligation is not always a simple issue even in classical law of obligations.

In the digital environment, this issue becomes more complex. If an obligation is fulfilled through a user account, electronic signature, platform or another digital mechanism, it must be determined whether the action was performed by the debtor, by a person authorised to act on the debtor's behalf, or by a third party who used the debtor's digital identity without authorisation. For that reason, digital fulfilment does not raise only the question whether performance occurred, but also the question to whom that performance may be attributed. In addition, Article 319 of the Law on Obligations provides that the debtor must perform the obligation, and the creditor must accept performance, at the place determined by the legal transaction or by law. In the digital environment, the place of performance may not always have the same importance as in the case of physical delivery of goods, but the regularity of performance remains equally important. In electronic payment, delivery of an electronic document, access to a digital service or delivery of digital content, proper fulfilment depends on whether the action was performed by the correct subject, in the agreed manner and at a time that can be reliably proved.

In the digital environment, contractual obligations are often fulfilled without direct contact between the parties. An obligation may be performed by electronic payment, delivery of an electronic document, enabling access to a digital service, delivery of digital content, activation of a user account, transfer of digital assets or another act performed through a digital platform. In such cases, fulfilment of the contract cannot be separated from the identity of the subject performing the action. In order to establish that the contractual obligation has been fulfilled, the digital action must be capable of being linked to the person who was obliged to perform it.

At this stage, digital identity performs the function of linking the contractual obligation to the contracting party. If a contract was concluded in the digital environment, legal certainty requires that subsequent acts of fulfilment can also be attributed to the appropriate subject. For example, in the provision of a digital service, it is important to determine whether access to the service was enabled for the correct user. In electronic delivery of a document, it is important to determine whether the document was delivered to the authorised recipient. In electronic payment, it is important to determine whether the payment originates from the debtor or from a person authorised to perform the obligation. In all these situations, the identification mechanism enables the legal connection between subject, digital action and fulfilment of the contractual obligation to be established.

This function builds on the role of digital identity at the stage of contract formation. If digital identity makes it possible to determine who made the offer and who accepted it, then at the stage of fulfilment it makes it possible to determine who performs the obligation arising from that contract. This ensures continuity between the creation of the contract and its fulfilment. Digital identity connects contractual will, contractual obligation and the act of fulfilment into a single legal relationship. It should therefore not be viewed only as a means of authentication at the moment of contract formation, but as an element that accompanies the entire contractual relationship in the digital environment.

Contract law traditionally proceeds from the rule that an obligation must be fulfilled as it is due and in accordance with the principles of good faith and fair dealing. In the digital environment, this rule acquires an additional dimension. It is not enough that a particular action has been performed, but it must be established whether it was performed by the appropriate subject, in a legally relevant manner and in accordance with the terms of the contract. If, for example, access to a digital service is enabled for the wrong user, if an electronic document is received by a person who is not the authorised recipient, or if a digital obligation is performed through a compromised account, the question may arise whether the obligation was properly fulfilled. Digital identity therefore also has an evidentiary function at the stage of fulfilment. Electronic traces created during performance may serve as evidence that a particular action was performed, when it was performed, in what manner and by which subject. Such traces may include records of electronic payment, electronic confirmations, system logs, electronic documents, electronic signatures, electronic time stamps or confirmations of electronic delivery. However, the legal value of these traces depends on their reliability and on the possibility of linking them to a

particular digital identity. The more reliable the connection between identity and act of fulfilment, the greater the possibility of proving proper fulfilment of the contractual obligation.

Trust services are particularly significant in this respect. An electronic signature may confirm the link between the signatory and an electronic document; an electronic seal may confirm the origin of a document issued by a legal person; an electronic time stamp may confirm the time at which a particular electronic action was created or sent; and qualified electronic delivery may contribute to proving receipt of a particular electronic document. These services do not change the nature of the contractual obligation, but they provide the legal and technical infrastructure for proving its fulfilment in the digital environment. In that sense, the normative regulation of electronic identification and trust services is directly relevant to the stage of contract fulfilment as well as to the stage of contract formation (European Parliament and Council, 2014; Law on Electronic Documents, Electronic Identification and Trust Services in Electronic Business, 2017/2021).

Electronic signatures, electronic seals and electronic time stamps therefore have direct importance at the stage of contract performance. An electronic signature may help prove who signed the document confirming fulfilment. An electronic seal may help establish that a document originates from a particular legal person. An electronic time stamp may be important for proving the moment of sending, receipt or performance of an electronic action. These mechanisms do not change the rules on fulfilment of obligations, but they allow those rules to be applied in the digital environment with a higher degree of evidentiary certainty.

Digital identity is also relevant to non-fulfilment of a contract. If a contracting party fails to perform an obligation, performs it late or performs it improperly, it is necessary to establish who is responsible for the breach. In the digital environment, these questions may be more complex because of unauthorised access, misuse of accounts, compromised authentication data or automated actions. If an action has been performed through the digital identity of one contracting party, the question arises whether that action can be attributed to that party or to a third person who misused the identity. The answer cannot be predetermined and cannot be based solely on the technical fact that a particular account was used. The circumstances of the specific case must be examined: the reliability of the identification system, the contractual rules on account use, the care exercised by the person whose identity was used, the ability of the other party to detect irregularity and the reasonableness of that party's reliance on the digital identity. In cases of

misuse of digital identity, the allocation of risk between the contracting parties becomes particularly important. The risk cannot always automatically be borne by the person whose identity was used, but neither can the other party that relied on that identity be protected without limitation. A legally relevant assessment must take into account good faith, due care, the reliability of the identification mechanism and the nature of the particular transaction. This connects digital identity not only with proof, but also with rules on liability and protection of a bona fide contracting party.

In this context, digital identity also has a responsibility-related function. It makes it possible to determine to whom a digital action may be attributed and who bears the consequences of its performance. This function is particularly important in digital transactions where actions are performed quickly, automatically or through platforms that themselves record the course of communication and performance. If a reliable system of identification and authentication exists, it is easier to determine whether the debtor performed the obligation, whether the creditor received performance and whether a breach of contract occurred. If such a system does not exist or is unreliable, the risk of dispute increases and proof of liability becomes more difficult.

The development of digital contracting shows that traditional institutes of the law of obligations must be applied in a new technological context. The rules on contract formation, fulfilment, delay, non-fulfilment and liability remain relevant, but their application depends on the possibility of reliably linking digital actions to particular subjects. Digital identity therefore does not change the basic structure of the obligation relationship, but it affects the way in which it is determined who is party to the contract, who is obliged to perform and who bears the consequences of non-fulfilment. This function of digital identity is one of the reasons why digital contracting should not be treated merely as a technical form of concluding contracts, but as a specific context for the application of traditional rules of contract law (Stojšić Dabetić & Mirković, 2022; Stojšić Dabetić & Mirković, 2024).

Digital identity therefore has at least three functions at the stage of contract fulfilment. The first is the individualisation of the debtor and the creditor. The second is evidentiary, because it enables the time, manner and subject of performance to be established. The third is responsibility-related, because it enables the consequences of non-fulfilment, delay or defective fulfilment to be attached to a particular contracting party. These functions are especially important where acts of performance are carried out through platforms, automated systems or user accounts, where the boundary between

technical access and legal action must not be oversimplified. Accordingly, digital identity does not change the rule that an obligation must be fulfilled in accordance with the contract and the law. It enables the legal order, in a digital environment, to determine who fulfilled the obligation, whether fulfilment was proper and to whom the consequences of fulfilment or non-fulfilment may be attributed. This is its specific function at the stage of fulfilment of contractual obligations.

Concluding remarks

The analysis shows that digital identity has an important contractual function in digital society. Its significance does not lie in creating a new and fully autonomous regime of contract law, but in enabling existing rules on contract formation, declarations of will, proof, legal attribution of digital actions and fulfilment of obligations to be applied in the digital environment.

Digital contracting does not abolish traditional institutes of the law of obligations. Offer, acceptance, agreement of wills, fulfilment of obligations and liability for breach of contract remain the basic categories of contract law. What changes is the way in which they are established and proved. When a declaration of will is made electronically, when a contract is concluded through a platform or when an obligation is fulfilled digitally, identity becomes directly connected with legal certainty.

The legal significance of digital identity does not arise from the mere fact that technology enables access to a system. It arises when the legal order recognises a particular digital action as capable of producing contractual legal effects. Digital identity must therefore be understood through the connection between the legal subject, the digital action and the legal consequence. The domestic, European and international normative framework confirms this direction of development. The Law on Electronic Commerce recognises the possibility of concluding contracts electronically, while at the same time providing for limitations on electronic form in certain legal transactions. The Law on Electronic Documents, Electronic Identification and Trust Services regulates the legal effect of electronic signatures, seals and time stamps. The eIDAS regime, Regulation (EU) 2024/1183 and the international instruments of UNCITRAL show that electronic identification, electronic communications and trust services are becoming part of the legal infrastructure of digital legal transactions.

Digital identity, therefore, does not displace classical institutes of the law of obligations. It makes them applicable in the digital environment. Its

basic legal significance lies in the fact that it enables digital communication not to remain merely a technical action, but to acquire legal meaning in relation to the formation, proof, legal attribution and fulfilment of contractual obligations.

REFERENCES

1. Biedermann, B., Scerri, M., Kozlova, V., & Ellul, J. (2024). A systematisation of knowledge: Connecting European digital identities with Web3. arXiv. https://arxiv.org/abs/2409.19032
2. CISG Advisory Council. (2003). Opinion No. 1: Electronic communications under CISG (C. Ramberg, Rapporteur). https://cisgac.com/wp-content/uploads/2024/10/CISG-AC-Opinion-No-1-Origianl-2003.pdf
3. Dukić Mijatović, M., & Mirković, P. (2022). Digital economy and information society – Scope and approach of legal regulation. Ekonomija: teorija i praksa, 15(2), 53–70. https://www.researchgate.net/publication/362032352_Digital_economy_and_information_society_scope_and_approach_of_legal_regulation
4. Durovic, M., & Lech, F. (2019). The enforceability of smart contracts. Italian Law Journal, 5(2), 493–511. https://theitalianlawjournal.it/data/uploads/5-italj-2-2019/493-durovic-lech.pdf
5. European Parliament and Council. (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. Official Journal of the European Union. https://eur-lex.europa.eu/eli/reg/2014/910/oj/eng
6. European Parliament and Council. (2024). Regulation (EU) 2024/1183 of the European Parliament and of the Council of 11 April 2024 amending Regulation (EU) No 910/2014 as regards establishing the European Digital Identity Framework. Official Journal of the European Union. https://eur-lex.europa.eu/eli/reg/2024/1183/oj/eng
7. Gabriel, H. D. (2006). The United Nations Convention on the Use of Electronic Communications in International Contracts: An overview and analysis. Uniform Law Review, 11(2), 285–303. https://doi.org/10.1093/ulr/11.2.285

8. Goodell, G., & Aste, T. (2019). A decentralized digital identity architecture. Frontiers in Blockchain, 2, Article 17. https://doi.org/10.3389/fbloc.2019.00017
9. Kaplane, A. (2025). The European Digital Identity Wallet: A new human right unlocked? Nordic Journal of Human Rights, 43(3), 304–316. https://doi.org/10.1080/18918131.2025.2551458
10. Mik, E. (2011). Evaluating the impact of the UN Convention on the Use of Electronic Communications in International Contracts on domestic contract law: The Singapore example. SSRN Electronic Journal. https://doi.org/10.2139/ssrn.2052995
11. Mirković, P. (2023). Digital assets – A legal approach to the regulation of the new property law institute. Pravo – teorija i praksa, 40(Special Issue), 17–31. https://doi.org/10.5937/ptp2300017M
12. Robles-Carrillo, M. (2024). Digital identity: An approach to its nature, concept, and functionalities. International Journal of Law and Information Technology, 32(1), Article eaae019. https://doi.org/10.1093/ijlit/eaae019
13. Sitouah, N., Esposito, M., & Bruschi, F. (2026). Self-sovereign identity and eIDAS 2.0: An analysis of control, privacy, and legal implications. arXiv. https://arxiv.org/abs/2601.19837
14. Stojšić Dabetić, J., & Mirković, P. (2022). Ugovaranje i ugovorno pravo u digitalnom društvu. Novi Sad: Pravni fakultet za privredu i pravosuđe. https://www.pravni-fakultet.edu.rs/downloads/naucni-rad/projekti/publikacije_prpsdd/UGOVARANJE_I_UGOVORNO_PRAVO_U_SAVREMENOM_DIGITALNOM_DRUSTVU.pdf
15. Stojšić Dabetić, J., & Mirković, P. (2024). Contracting in the digital society – Certain issues of significance in regards to regulation of offers and acceptance of offers in e-contracts. Kultura polisa, 21(1), 181–201. https://kpolisa.com/index.php/kp/article/view/1505
16. Stojšić Dabetić, J., Mirković, P., & Aleksić Oliveira, N. (2025). The emergence of digital identity as a new legal concept. Pravo – teorija i praksa, 42(3), 21–34. https://doi.org/10.5937/ptp2503021M
17. Sullivan, C. L. (2011). Digital identity: An emergent legal concept. University of Adelaide Press. https://library.oapen.org/handle/20.500.12657/33171
18. UNCITRAL. (1996). UNCITRAL Model Law on Electronic Commerce with Guide to Enactment 1996. United Nations. https://uncitral.un.org/en/texts/ecommerce/modellaw/electronic_commerce

19. UNCITRAL. (2001). UNCITRAL Model Law on Electronic Signatures with Guide to Enactment 2001. United Nations. https://uncitral.un.org/en/texts/ecommerce/modellaw/electronic_signatures
20. United Nations. (2005). United Nations Convention on the Use of Electronic Communications in International Contracts. United Nations Commission on International Trade Law. https://uncitral.un.org/en/texts/ecommerce/conventions/electronic_communications
21. Law on Electronic Commerce, Official Gazette of the Republic of Serbia, Nos. 41/2009 95/2013 and 52/2019. https://www.paragraf.rs/propisi/zakon_o_elektronskoj_trgovini.html
22. Law on Electronic Documents, Electronic Identification and Trust Services in Electronic Business, Official Gazette of the Republic of Serbia, Nos. 94/2017 and 52/2021. https://www.paragraf.rs/propisi/zakon-o-elektronskom-dokumentu-elektronskoj-identifikaciji-i-uslugama-od-poverenja-u-elektronskom-poslovanju.html
23. Law on Obligations, Official Gazette of the SFRY, Nos. 29/1978, 39/1985, 45/1989 - decision of the Constitutional Court of Yugoslavia and 57/1989; Official Gazette of the FRY, No. 31/1993; Official Gazette of Serbia and Montenegro, No. 1/2003 - Constitutional Charter; and Official Gazette of the Republic of Serbia, No. 18/2020. https://www.paragraf.rs/propisi/zakon_o_obligacionim_odnosima.html