COMMERCIAL CONTRACTS IN THE DIGITAL ERA: LEGAL CHALLENGES AND THE SECURITY OF ELECTRONIC TRANSACTIONS

Nermine ISMAILI[1], Sheherzada MURATI[1]
[1] *University of Tetova "Fadil Sulejmani", Tetovo, North Macedonia*
Corresponding author: nermine.ismaili@unite.edu.mk

Abstract

Electronic contracts have today become a common form of commercial relations, and their development in recent years has been exceptionally rapid. The shift from the written document to digital data has not been merely a technical change; it has also put to the test some of the fundamental principles of the law of obligations: form, the expression of consent, the identification of the parties and proof. This paper aims to analyse how the law responds to these challenges and how secure trade conducted by electronic means really is. It approaches the problem from two perspectives. The first part examines the validity of the electronic contract: the principle of functional equivalence established by the UNCITRAL instruments, the moment at which a contract is concluded in the online environment, the law applicable to cross-border relations and the legal position of smart contracts. The second part, in turn, focuses on the security of transactions, namely on electronic signatures and trust services under the eIDAS Regulation and its 2024 amendments, on strong customer authentication in electronic payments and on the protection of personal data. The study relies on the normative and comparative method, with a particular focus on North Macedonia. Its 2019 Law on Electronic Documents, Electronic Identification and Trust Services, amended in 2025 to introduce a digital identity wallet, represents an important step towards harmonisation, even though full connection to the European Digital Identity Wallet is planned only for 2027. The main conclusion is that contract law has shown a good capacity to adapt, while the greatest challenge today is not legal in the narrow sense but concerns trust in the technical infrastructure. Bringing Macedonian legislation into line with EU law would strengthen this trust among businesses and consumers alike.

Keywords: *functional equivalence, electronic signature, trust services, eIDAS, smart contracts, North Macedonia*

1. Introduction

Contract law is one of the oldest and most stable branches of private law, yet few fields have been affected by digitalisation as profoundly as this one. Commercial relationships that for centuries relied on physical documents and on the presence of the parties are now built through platforms, applications and automated systems. For companies, this brings savings in time and costs, as well as the opportunity to enter distant markets. For lawyers, however, such a development opens new challenges and a series of questions, because the traditional concepts of civil law, such as the written form, the manifestation of will and the original document, were created for an entirely different reality.

In response to these changes, the first answer came from international law. In 1996, UNCITRAL adopted the Model Law on Electronic Commerce, under which information may not be denied legal effect solely on the grounds that it is in electronic form. This principle was reaffirmed in the United Nations Convention on the Use of Electronic Communications in International Contracts, adopted in 2005.[1] The European Union went a step further. The Electronic Commerce Directive required Member States to ensure that their legal systems allow contracts to be concluded by electronic means,[2] while the eIDAS Regulation of 2014, substantially supplemented in 2024, established common rules on electronic signatures, seals

[1] UNCITRAL Model Law on Electronic Commerce with Guide to Enactment 1996, with additional article 5 bis as adopted in 1998 (New York: United Nations, 1999), Article 5; United Nations Convention on the Use of Electronic Communications in International Contracts, adopted by the General Assembly on 23 November 2005 (resolution 60/21), Article 8(1).

[2] Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market, OJ L 178, 17 July 2000, Article 9(1).

and other trust services.[3] North Macedonia followed this model with its Law on Electronic Commerce of 2007 and, later, with its Law on Electronic Documents, Electronic Identification and Trust Services of 2019.[4]

However, even with the adoption of these laws, it cannot be said that all dilemmas have been resolved. Domestic legal literature points out that the electronic contract has redefined the traditional notions of contract law, such as the stages of reaching an agreement, the form of the contract and the manner of its performance.[5] The most complex issues arise with smart contracts, in which obligations are performed automatically by a computer program. Although some have presented them as an alternative to contract law, a number of the most serious studies, as well as the Law Commission of England and Wales, reach the conclusion that existing rules are capable of dealing with such contracts and that smart contracts cannot replace contract law itself.[6] For North Macedonia, the question remains open whether smart contracts require a special law or the amendment of existing legislation.[7]

From this perspective, the paper seeks to reflect the complexity of two main questions. The first concerns whether the existing rules are sufficient to guarantee the validity of commercial contracts concluded by electronic means. The second refers to the legal tools that make such trade secure, and to the extent to which Macedonian legislation has adopted them. To answer these questions, Section 2 explains the essence of the electronic contract and the way in which it is concluded. Section 3 addresses the main legal challenges, Section 4 the mechanisms for the security of transactions, Section 5 the situation in North Macedonia, and Section 6 summarises the conclusions and recommendations.

2. The Electronic Contract: Concept and Formation

The electronic contract does not represent a new type of contract, but only a new way of concluding one. What distinguishes it from the traditional contract is not the content of the rights and obligations of the parties, but the means through which their will is expressed. The UNCITRAL Model Law defines a data message as information generated, sent, received or stored by electronic, optical or similar means, including electronic data interchange and electronic mail.[8] On this basis, the same instrument provides that an offer and its acceptance may be expressed by means of such messages, and that a contract may not be denied validity solely because such messages were used in its formation.[9] The 2005 Convention follows the same approach and refers to "electronic communications", a term broad enough to cover any form of digital exchange between the parties.[10] Accordingly, an electronic contract may be an agreement concluded by e-mail, an agreement concluded with a click on a trader's website, or one that is performed automatically by a computer program.

In practice, the most important issue is determining the moment at which the contract is formed, that is, when it is considered concluded. The 2005 Convention provides that an electronic communication is deemed to be received when it becomes capable of being retrieved by the

[3] Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market, OJ L 257, 28 August 2014; 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, OJ L, 2024/1183, 30 April 2024.

[4] Law on Electronic Commerce, Official Gazette of the Republic of Macedonia No. 133/2007; Law on Electronic Documents, Electronic Identification and Trust Services, Official Gazette of the Republic of North Macedonia Nos. 101/2019, 275/2019, 3/2025 and 135/2025.

[5] Igor Kambovski, 'The Law on Electronic Commerce – Ten Years Later', *Collection of Papers of the Faculty of Law, Niš* 57, no. 81 (2018), pp. 265–266.

[6] Kevin Werbach and Nicolas Cornell, 'Contracts Ex Machina', *Duke Law Journal* 67 (2017), p. 313; Law Commission, *Smart Legal Contracts: Advice to Government*, Law Com No 401 (London, 25 November 2021).

[7] Mirjana Ristovska, 'Smart (Legal) Contracts: New Challenge for North Macedonian Legal System', in *Law in the Age of Digital Technologies* (Milano: Milano University Press, 2025), p. 180.

[8] UNCITRAL Model Law on Electronic Commerce, Article 2(a).

[9] Ibid., Article 11(1).

[10] United Nations Convention on the Use of Electronic Communications in International Contracts, Article 4(b).

addressee at an electronic address designated by that addressee.[11] The Convention further clarifies that a proposal which is not addressed to one or more specific parties, such as offers made on websites, is in principle to be considered an invitation to make offers rather than a binding offer.[12] EU law, for its part, requires traders to inform buyers, before the order is placed, of the technical steps leading to the conclusion of the contract, and to acknowledge receipt of the order without undue delay.[13] Under Macedonian law, an electronic contract is considered concluded at the moment when the offeror receives the acceptance of the offer. This solution preserves the classic principle of the law of obligations, but applies it in an environment where offer, acceptance and performance are often separated in time.[14]

When speaking of electronic contracts, it is important to distinguish between contracts concluded between traders and those concluded with consumers. In the former, the parties enjoy broad freedom to regulate the means of communication themselves, and the provisions on information and on the acknowledgement of the order may be excluded by agreement.[15] In the latter, EU law lays down stricter rules in order to protect the weaker party. Thus, where a distance contract is concluded through a website, the order button must be labelled clearly with the words "order with obligation to pay" or a similar unambiguous formulation, so that the consumer is aware of assuming an obligation.[16] In addition, the consumer has the right to withdraw from the contract within 14 days without giving any reason.[17] Therefore, for the European legislator, the mere recognition of the electronic form of the contract is not sufficient; it also requires an additional guarantee to be provided for the party that has less knowledge and less power in the relationship.

3. Legal Challenges

The first challenge facing legal science concerns the form of the contract. A number of legal systems require that a contract be concluded in written form and signed by the parties, whereas in the electronic environment there is neither paper nor a handwritten signature. The UNCITRAL Model Law addresses this challenge through the principle of functional equivalence. The requirement of written form is met if the information is accessible so as to be usable for subsequent reference,[18] while the requirement of a signature is met if a method is used to identify the person, to indicate that person's approval of the content, and if that method is sufficiently reliable.[19] The eIDAS Regulation goes further and distinguishes three levels of electronic signature: simple, advanced and qualified.[20] Only a qualified electronic signature has a legal effect equivalent to that of a handwritten signature, while other signatures may not be denied legal effect and admissibility as evidence in legal proceedings solely on the grounds that they are in electronic form.[21] In other words, their evidentiary weight is left to national courts, and it is precisely from here that uncertainty arises for the parties to commercial contracts.

The second challenge concerns the identity of the parties. Whereas in a traditional contract the parties usually meet or know each other, on the internet the trader often does not know with certainty who exactly is on the other side of the screen. This creates uncertainty and

[11] Ibid., Article 10(2).
[12] Ibid., Article 11.
[13] Directive 2000/31/EC, Articles 10(1)(a) and 11(1).
[14] Kambovski, 'The Law on Electronic Commerce – Ten Years Later', p. 266.
[15] Directive 2000/31/EC, Articles 10(1) and 11(1)–(2), which apply "except when otherwise agreed by parties who are not consumers".
[16] Directive 2011/83/EU of the European Parliament and of the Council of 25 October 2011 on consumer rights, OJ L 304, 22 November 2011, Article 8(2).
[17] Ibid., Article 9(1).
[18] UNCITRAL Model Law on Electronic Commerce, Article 6(1).
[19] Ibid., Article 7(1).
[20] Regulation (EU) No 910/2014, Article 3(10)–(12).
[21] Ibid., Article 25(1)–(2).

automatically affects the location of the parties as well, which is important for determining the applicable law and the competent court. The 2005 Convention provides that a party's place of business is not determined merely by the location of the equipment and technology supporting its information system, nor merely by a domain name or electronic mail address connected to a specific country.[22] To reduce this risk, the eIDAS Regulation established a system of mutual recognition of electronic identification means between Member States, with three assurance levels: low, substantial and high.[23] With the 2024 amendments, each Member State is required to provide its citizens with at least one European Digital Identity Wallet.[24] In this way, the identification of the parties is gradually shifting from a simple declaration by the user to a digital identity verified by the state.

The third challenge that arises in electronic contracting is that the parties are often located in different states. While the internet knows no borders, contract law remains largely national, and it is therefore important to determine which law will apply to a given relationship. In the European Union, this issue is governed by the Rome I Regulation, under which the parties are free to choose the applicable law themselves. Where they have made no choice, a contract for the sale of goods is governed by the law of the country where the seller has its habitual residence. In consumer contracts, however, the law of the country where the consumer has his or her habitual residence applies in principle, provided that the trader directs its activities to that country, and a choice of another law may not deprive the consumer of the protection afforded by that law.[25] The Court of Justice of the EU has clarified that the mere fact that a trader's website is accessible from another state is not in itself sufficient to consider that its activity is directed to that state; other indicators are required, such as the language, the currency or the international dialling code.[26] This shows that a trader selling online must know in advance which law it may have to face.

The fourth and perhaps most sensitive challenge facing the legal world today concerns smart contracts. The Law Commission of England and Wales defines them as legally binding contracts in which some or all of the obligations are defined in and/or performed automatically by a computer program.[27] The main problem lies not in their validity, but in the way they are enforced. When the predetermined condition is met, the program performs the obligation by itself, and the parties have no way of stopping the execution even if there has been an error in the code, a fraud or a change of circumstances. As a result, instead of bringing certainty, the contract may produce unjust consequences, which can only be remedied after they have occurred. It is precisely for this reason that the European Law Institute has proposed the principle that consumer protection rules prevail over coded transactions and fully govern them.[28] Put differently, technology may serve as an auxiliary tool, but it cannot replace the law. It can facilitate the performance of the contract, but liability, interpretation and the protection of the injured party remain the task of the law.[29]

[22] United Nations Convention on the Use of Electronic Communications in International Contracts, Article 6(4)–(5).
[23] Regulation (EU) No 910/2014, Articles 6 and 8(2).
[24] Regulation (EU) No 910/2014, as amended by Regulation (EU) 2024/1183, Article 5a(1).
[25] Regulation (EC) No 593/2008 of the European Parliament and of the Council of 17 June 2008 on the law applicable to contractual obligations (Rome I), OJ L 177, 4 July 2008, Articles 3(1), 4(1)(a) and 6(1)–(2).
[26] Joined Cases C-585/08 and C-144/09, *Peter Pammer v Reederei Karl Schlüter GmbH & Co. KG* and *Hotel Alpenhof GesmbH v Oliver Heller*, Judgment of 7 December 2010, ECLI:EU:C:2010:740, paras 69 and 93.
[27] Law Commission, *Smart Legal Contracts: Advice to Government*, Law Com No 401 (London, 25 November 2021), para. 2.11.
[28] European Law Institute, *ELI Principles on Blockchain Technology, Smart Contracts and Consumer Protection* (Vienna: ELI, 2023), Principle 13, p. 40.
[29] Werbach and Cornell, 'Contracts Ex Machina', p. 313.

4. Security of Electronic Transactions

Since the previous section dealt with the electronic contract and its validity, the question that still remains open is how the parties can trust such a contract. The answer is provided by the system of trust services, which the eIDAS Regulation defines as electronic services that include, among others, the creation and validation of electronic signatures and seals, electronic time stamps, electronic registered delivery and certificates for website authentication.[30] Their legal significance lies in the presumptions they create. A qualified electronic seal enjoys the presumption of the integrity of the data and of the correctness of their origin,[31] while a qualified electronic time stamp enjoys the presumption of the accuracy of the date and time it indicates.[32] In practice, this means that the party relying on a qualified service does not need to prove itself that the document has remained unchanged, since the burden of proof lies with the party contesting it. To guarantee this reliability, qualified providers of these services are regularly audited by independent bodies at least every 24 months.[33]

The security of an electronic contract does not end with the conclusion of the contract itself, since the most sensitive part of the transaction is usually the payment. For this reason, the second EU Payment Services Directive (PSD2) requires payment service providers to apply strong customer authentication when the customer accesses his or her payment account online, initiates an electronic payment transaction, or carries out any action through a remote channel which may imply a risk of fraud.[34] Strong customer authentication is based on at least two independent elements from different categories: something only the user knows (such as a password), something only the user possesses (such as a phone) and something the user is (such as a fingerprint).[35] This requirement also has direct consequences for liability. If the payment service provider does not require strong customer authentication, the payer does not bear any financial loss unless he or she has acted fraudulently.[36] In this way, the risk of the transaction is transferred to the party with the greater technical capacity to prevent it.

Every electronic contract also involves the processing of personal data: the name, the address, the bank card number and the purchase history. The General Data Protection Regulation (GDPR) permits such processing without separate consent where it is necessary for the performance of the contract.[37] However, the same act obliges traders and service providers to implement appropriate technical and organisational measures to ensure the security of the data, such as encryption and pseudonymisation.[38] Where a security breach occurs, the controller must notify the supervisory authority without undue delay and, where feasible, within 72 hours of becoming aware of it.[39] Failure to comply with these obligations may be sanctioned by administrative fines of up to EUR 10 million or up to 2% of the undertaking's total worldwide annual turnover.[40] In this way, data protection does not concern only the privacy of the parties, but also becomes an integral part of the security of the commercial transaction itself.

[30] Regulation (EU) No 910/2014, Article 3(16).
[31] Ibid., Article 35(2).
[32] Ibid., Article 41(2).
[33] Ibid., Article 20(1).
[34] Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market (PSD2), OJ L 337, 23 December 2015, Article 97(1).
[35] Ibid., Article 4(30).
[36] Ibid., Article 74(2).
[37] 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 (General Data Protection Regulation), OJ L 119, 4 May 2016, Article 6(1)(b).
[38] Ibid., Article 32(1)(a).
[39] Ibid., Article 33(1).
[40] Ibid., Article 83(4)(a).

5. The Legal Framework in North Macedonia

By following developments in EU law, North Macedonia has gradually built its framework for electronic commerce. The first step was the Law on Electronic Commerce of 2007, adopted at a time when there were only a few online stores on the domestic market.[41] This law achieved partial harmonisation with Directive 2000/31/EC, while the amendments proposed in 2010 were aimed at full harmonisation with it.[42] The second and more important step came with the 2019 Law on Electronic Documents, Electronic Identification and Trust Services, which is aligned with the eIDAS Regulation and distinguishes between qualified and non-qualified trust services.[43] This law was supplemented in 2025 with rules on the digital wallet for electronic identity.[44] Thus, the domestic legislator is not satisfied with formal harmonisation alone, but strives to keep pace with European developments.

The process of harmonisation was not limited to electronic signatures and documents. In February 2020, North Macedonia adopted a new Law on Personal Data Protection, which is aligned with the General Data Protection Regulation (GDPR).[45] Two years later, the Law on Payment Services and Payment Systems was adopted, which harmonises domestic legislation with the PSD2 Directive and defines strong authentication as the confirmation of identity through at least two independent elements: knowledge, possession and inherence.[46] However, the practical application of this obligation began almost four years later. According to the Macedonian Banking Association, strong customer authentication in electronic payments only began to apply from 1 March 2026.[47] This shows that, in practice, a long period often passes between the adoption of a law and its implementation, which leaves the parties to electronic contracts less protected.

Although visible progress can be observed in this field, the legal framework of the Republic of North Macedonia still remains incomplete. The first gap in this respect concerns smart contracts, which to this day are still not expressly regulated by any domestic law. The question has been raised in the literature whether a special law should be adopted for them or whether the existing laws should be supplemented, in particular the Law on Obligations and the Law on Electronic Commerce.[48] The second gap, meanwhile, affects digital identity. Although the law already recognises the digital wallet, under the Reform Agenda its pilot phase, with at least ten public electronic services, is planned by December 2026, while full participation in the European Digital Identity Wallet is foreseen only by December 2027.[49] This leads us to understand that, in practice, until 2027 Macedonian traders and consumers will not be able to use the same means of identification as their partners in the EU, which will make the conclusion of cross-border electronic contracts more difficult.

[41] Kambovski, 'The Law on Electronic Commerce – Ten Years Later', p. 259.
[42] Ministry of Economy of the Republic of Macedonia, *Proposal for a Law Amending the Law on Electronic Commerce* (Skopje, October 2010), Introduction, Section I.
[43] Law on Electronic Documents, Electronic Identification and Trust Services, Official Gazette of the Republic of North Macedonia No. 101/2019, footnote to the title (harmonisation with Regulation (EU) No 910/2014, CELEX 32014R0910).
[44] Law Amending the Law on Electronic Documents, Electronic Identification and Trust Services, Official Gazette of the Republic of North Macedonia No. 135/2025, 4 July 2025.
[45] Law on Personal Data Protection, Official Gazette of the Republic of North Macedonia No. 42/2020, footnote to the title (harmonisation with Regulation (EU) 2016/679, CELEX 32016R0679).
[46] Law on Payment Services and Payment Systems, Official Gazette of the Republic of North Macedonia No. 90/2022, footnote to the title (harmonisation with Directive (EU) 2015/2366) and Article 2(1), point 41.
[47] Macedonian Banking Association, 'From 1 March 2026, Strong Customer Authentication in Electronic Payments Begins to Apply', *bankarstvo.mk* (accessed 1 November 2026).
[48] Ristovska, 'Smart (Legal) Contracts: New Challenge for North Macedonian Legal System', p. 180.
[49] 'Телефонот станува лична карта, ЕУ сака дигитален идентитет' [The Phone Becomes an ID Card: The EU Wants a Digital Identity], *trn.mk*, 24 September 2026.

6. Conclusion

The analysis carried out so far also reflects the answer to the first question raised at the outset, which is largely positive. On the basis of the principle of functional equivalence, established by the UNCITRAL instruments and accepted at the same time by EU law, a contract concluded in electronic form is no less valid than one concluded on paper. However, this formal validity does not resolve all the problems faced by the parties to electronic contracts. The evidentiary weight of non-qualified electronic signatures remains within the competence of national courts, the identification of the parties remains uncertain, the applicable law in cross-border relations requires particular care, while smart contracts raise questions to which there are still no clear answers. The answer to the second question is likewise two-sided. In its law, the EU has created effective tools for the security of transactions, such as trust services with their presumptions, strong customer authentication and data protection obligations, and North Macedonia has adopted the same tools, but their implementation in practice comes with considerable delay.
From the above, several recommendations can be drawn for the competent institutions in North Macedonia. First, the Law on Obligations and the Law on Electronic Commerce should be supplemented with provisions clarifying the legal position of smart contracts, particularly with regard to the moment of conclusion, the interpretation of code and liability where automated execution causes damage. Second, priority should be given to integration into the European Digital Identity Wallet, so as to accelerate the processes through which domestic entities can identify themselves and sign contracts with partners from the EU on equal terms. Third, judges need to be trained in assessing electronic evidence and electronic signatures, so that case law becomes uniform and predictable. Fourth, the period between the adoption of laws and their implementation in practice should be shortened, with clear deadlines and effective supervision by the competent institutions. Finally, an overarching conclusion would be that electronic commerce will develop and progress soundly only when law and technology move forward together, with neither competing against the other.

References

[1] Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce). OJ L 178, 17 July 2000.
[2] Directive 2011/83/EU of the European Parliament and of the Council of 25 October 2011 on consumer rights. OJ L 304, 22 November 2011.
[3] Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market (PSD2). OJ L 337, 23 December 2015.
[4] European Law Institute. *ELI Principles on Blockchain Technology, Smart Contracts and Consumer Protection*. Vienna: European Law Institute, 2023.
[5] Joined Cases C-585/08 and C-144/09, *Peter Pammer v Reederei Karl Schlüter GmbH & Co. KG* and *Hotel Alpenhof GesmbH v Oliver Heller*. Judgment of the Court (Grand Chamber) of 7 December 2010, ECLI:EU:C:2010:740.
[6] Kambovski, Igor. "The Law on Electronic Commerce – Ten Years Later." *Collection of Papers of the Faculty of Law, Niš* 57, no. 81 (2018): 259–268.
[7] Law Commission. *Smart Legal Contracts: Advice to Government*. Law Com No 401. London, 25 November 2021.
[8] Law on Electronic Commerce. Official Gazette of the Republic of Macedonia No. 133/2007.
[9] Law on Electronic Documents, Electronic Identification and Trust Services. Official Gazette of the Republic of North Macedonia Nos. 101/2019, 275/2019, 3/2025 and 135/2025.
[10] Law on Payment Services and Payment Systems. Official Gazette of the Republic of North Macedonia No. 90/2022.
[11] Law on Personal Data Protection. Official Gazette of the Republic of North Macedonia No. 42/2020.
[12] Macedonian Banking Association. "From 1 March 2026, Strong Customer Authentication in Electronic Payments Begins to Apply." *bankarstvo.mk*. Accessed 1 November 2026.

[13] Ministry of Economy of the Republic of Macedonia. *Proposal for a Law Amending the Law on Electronic Commerce*. Skopje, October 2010.
[14] Regulation (EC) No 593/2008 of the European Parliament and of the Council of 17 June 2008 on the law applicable to contractual obligations (Rome I). OJ L 177, 4 July 2008.
[15] 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 (eIDAS). OJ L 257, 28 August 2014.
[16] 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 (General Data Protection Regulation). OJ L 119, 4 May 2016.
[17] 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. OJ L, 2024/1183, 30 April 2024.
[18] Ristovska, Mirjana. "Smart (Legal) Contracts: New Challenge for North Macedonian Legal System." In *Law in the Age of Digital Technologies*, 169–181. Milano: Milano University Press, 2025.
[19] "Телефонот станува лична карта, ЕУ сака дигитален идентитет" [The Phone Becomes an ID Card: The EU Wants a Digital Identity]. *trn.mk*, 24 September 2026.
[20] UNCITRAL. *UNCITRAL Model Law on Electronic Commerce with Guide to Enactment 1996, with additional article 5 bis as adopted in 1998*. New York: United Nations, 1999.
[21] United Nations Convention on the Use of Electronic Communications in International Contracts. Adopted by the General Assembly on 23 November 2005 (resolution 60/21).
[22] Werbach, Kevin, and Nicolas Cornell. "Contracts Ex Machina." *Duke Law Journal* 67 (2017): 313–382.