Mirković Predrag
https://orcid.org/0000-0003-2323-040X

Stojšić Dabetić Jelena
https://orcid.org/0000-0002-3229-837X

Aleksić Oliveira Nina
https://orcid.org/0009-0004-9482-3012

UDK: 347.121:004.9
Original scientific paper
DOI: 10.5937/ptp2503021M
Received on: April 15, 2025
Approved for publication on:
May 24, 2025
Pages: 21–34

THE EMERGENCE OF DIGITAL IDENTITY AS A NEW LEGAL CONCEPT

ABSTRACT: With the development of modern digital society, the degree of interaction among subjects taking place in the digital space is increasing. This interaction is based on the use of personal data between subjects for the purpose of confirming and verifying their identity. The issue of applying personal identity in the digital space has created the reality of the *de facto* existence of digital identity as a new form of personal identification. Digital identity is an identity composed of information stored and transmitted in digital form. Therefore, the question arises as to how the new concept of personal identity, as digital identity, can be encompassed by legal rules in order to enable transactions. The authors argue that digital technology calls for a new philosophy of identity. They further argue that digital identity necessarily requires a redefinition of the traditional legal framework. In the following discussion, the paper will examine who may be treated as a legal subject in transactions conducted through digital identity. It will also consider how legal presumptions may change to include new realities, and,

* LLD, Full Professor, University Business Academy in Novi Sad, Faculty of Law for Commerce and Judiciary in Novi Sad, Novi Sad, Serbia, e-mail: mirkovic@pravni-fakultet.info

** LLD, Associate Professor, University Business Academy in Novi Sad, Faculty of Law for Commerce and Judiciary in Novi Sad, Novi Sad, Serbia, e-mail: j.stojsic.dabetic@pravni-fakultet.info

*** LLD, Assistant Professor, University Business Academy in Novi Sad, Faculty of Law for Commerce and Judiciary in Novi Sad, Novi Sad, Serbia, e-mail: nina.aleksic@pravni-fakultet.info

most importantly, it will present the legal treatment of the technical structure that constitutes digital identity.

Keywords: *digital identity, transactional identity, personal data, legal transactions, registered identity, digital citizenship.*

1. Introduction

Personal identity is a traditional and established legal institute that serves for the legally secure identification of subjects in legal transactions. With the emergence of digital space as surroundings for legal transactions, personal identity has showed itself with limited reach for the needs of interaction. However, the frequency of the usage of personal identity in digital space is reflection of its importance for the digital society.

With the development of modern society as digital, the degree of interaction of subjects that takes place in the digital space is increasing, both in form of interaction of legal and natural persons with public authorities, as well as their mutual interaction. The interaction that takes place in digital transactions and digital economy is based on the usage of personal data between subjects, in order to confirm and verify their identity. The issue of the application of personal identity in the digital space has created the reality of de facto existence of digital identity as a new form of personal identification (Zwitter, Gstrein & Yap, 2020). Digital identity (DI) is an identity which is composed of information stored and transmitted in digital form. A specific DI is now emerging as governments around the world move their services and transactions on-line, taking steps towards providing digital identities to their beneficiaries.

So, the question emerges as to how can new concept of personal identity as digital identity be comprehended by the legal rules, in order to enable transactions? We argue that digital technology invokes new philosophy of identity. We also argue that digital identity as necessity redefines traditional law framework. In the following discussion in this paper, we will see who can be treated as legal subject in transactions that are conducted via digital identity. We shall discuss how can legal presumptions alter to include new realities. And most important, we shall present legal treatment of technical structure that digital identity is comprised of. The paper will present and analyze doctrinal points of view regarding the legal treatment of personal identity in digital space as digital identity, with the aim of providing legal

understanding for changes that digital economy inevitably brings. The aim of the paper is to further clarify changes that the law must undergone in order to keep pace with the development of digital society.

2. Digitalization of government transactions and data-driven economy

Digital or computer technology is today embedded in processes fundamental to economic and social order and has positioned itself as a whole new and primary environment for interaction. Modern digital economy makes individuals, businesses and governments increasingly dependent on technology in their transactions, as well as their daily tasks. Compared to just a few years ago, it is now a relatively common occurrence to be asked for proof of identity for transactions which take place on-line. Digital age made new technologies as primary mediators for identity verification and identification of individuals.

A transaction, in the sense of legal relations, is a relationship for which an individual or a natural person, must prove his identity, whether it takes place in person (face to face) or through other forms of communication. The identity for the purposes of transactions, which is designated as a transactional identity, implies the usage in order to establish a relationship between an individual and a state authority or a commercial entity, and it can be for the purpose of just an inquiry or for the purpose of conclusion of a contract, but does not include non-business interactions (such as social networks or social interactions).

In modern society emerges the new legal concept of identity that consists of database identity and the subset of information that is identity used for transactions with government or inter-partes. As dealings previously conducted in-person are replaced by dealings conducted without a history of personal acquaintance, and frequently without person to person interaction, the requirement to establish identity for transactional purposes has increased (Dash & Sharma, 2021, p. 2). Digital identity (DI) is the means by which an individual is recognised and can transact in the digital realm, digital identity becomes individual's officially recognized identity for transactional purposes.

A specific DI is now emerging as governments around the world move their services and transactions on-line. States across the world are taking steps towards digitalization of their public distribution systems which are based on providing digital identities to beneficiaries. State-led and public–private

initiatives use technology to provide official identification, to control and secure external borders, and to distribute humanitarian aid to populations in need. Digital identity is emerging as a distinct new legal concept in countries that move to fully digitalize government transactions. This new form of identity is the primary means by which a natural person can access these services. This is a fundamental principle of e-government as many countries now require that an individual must have a digital identity to access government services and for transactions with government departments and agencies. These schemes are significant because they establish one identity, initially for use in transactions with government, but with the long-term consequence of also extending to transactions with the private sector (Sullivan, 2013, p. 125). In the context of using state services, the concept of "one person, one identity" prevails precisely in order to reduce the possibility of abuse. In the domain of private communications, this need is not so pronounced and it is common for a person to have multiple identities for the purposes of communication and using different platforms.

Further in the paper, we will show that in the modern digital society and within the electronic transactions of the data-driven economy, a new legal concept of identity is emerging which is made up exclusively of a corpus of information or data and which the law has recognized as a legal subject, and which aims to redefine the legal understanding of the identity of individuals. Within computer science, information or data has its own function and meaning, and machine intelligence can make decisions and in that context act like a human being, bearing in mind the effects of that in real life.

3. Redefining personal identity in digital society – new philosophy of identity

Identity, in the context of DI, is an essential legal concept, related to individual elements of a legal or natural person that are provided by regulations as elements that make up and on the basis of which identity is determined. Digital identification means identification on the Internet in the form of a group of different data such as username, first name, last name, e-mail address, place of residence or a combination of other data that uniquely describe us. This data stored on networks constitutes a digital identity such as a web or network identity that an individual, organization or electronic device possesses to enter cyberspace. Digital identity is an identity which is composed of information stored and transmitted in digital form. DI is all the information digitally recorded about an individual. It is arguable if an

individual can have more than one DI. Digital identity has its significant implications in both commercial and legal surroundings, which must be accompanied by the adequate normative framework. Legal professions are in ongoing process of finding ways to adequately protect this new concept of identity as well as legal interests of individuals intertwined (Bwana, 2024, pp. 84–85). It is the task of the lawmakers to find an effective way to regulate rights and duties arising from digital identity, while effectuating both the legal and commercial significance of DI.

Identity in the sense of a legal concept means a set of digitally stored and transferable information, in the sense of an "identity database", which has been given legal force, i.e. recognized a specific legal effect through a specific state regulation. Access is provided under certain conditions. Digital identity means an identity that consists of information that is stored and transmitted digitally, that is, that was created in digital form or exists in such a form, and is transmitted and handled in this way. Access to the information that makes up the digital identity implies certain procedural steps, the so-called „access schemes" in the technological sense. In the context of the digital society, or digital environment (the so-called digital space), information as a concept also includes data, in the sense that every piece of information about a legal or natural person is considered information, but not every piece of information is considered data. On the other hand, in the context of the digital space of the digital society, data is a legally regulated concept with its own special legal regime of protection. Identification of individuals for the purposes of using digital services is called authentication and is a prerequisite for access to digital content, and is done through a username and password, a one-time SMS password, a fingerprint, and a digital certificate. Authentication is based, in a technical sense, usually on at least two mutually independent elements: something only the user has (e.g. phone or smart card), something only the user knows (e.g. PIN code or password), and something that uniquely identifies the user (e.g. fingerprint or iris).

In the technical sense, digital identity consists of two levels - the so-called. transactional identity, which implies a smaller volume, but precisely defined, of information with which the transaction is carried out, or interaction, and only after their presentation in the prescribed manner, and the so-called other information, which is larger in scope and contains additional data and information (registered identity). Transactional identity, as a part of DI, is its essential part, but at the same time a static part because it rests on information and data that are not of a variable character, or are not subject to frequent changes - full name, gender, date of birth and usually one "identifying" piece of information such as

a signature or numerical sequence, image or biometric data (fingerprint, pupil) is added to them (Finck, 2018, p. 25). The identifying information has the role of enabling the transactional identity to connect the entire DI with a certain individual, through an appropriate technical authentication process that takes place on a certain platform where the registered digital identity is registered. The matching of this information for the purposes of interaction in the digital space is what is the subject of personal data protection, for example, the transactional part of the DI is private, while the data that forms the DI is mostly public and are freely used and disposed of by the individual in public, i.e. they are not subject to strict privacy protection (Wang & De Filippi, 2020, pp. 3–4). In this sense, transactional identity is a gate-keeper and a barrier to access to other information. The information that makes up the registered identity is broader in its scope than the information on which the transactional identity rests, it is not usually part of the public domain and is subject to protection under the rules on the protection of privacy or personal data. This set of information is accessed through a transactional identity, i.e. by entering information that is part of the transactional identity. Thus, digital identity consists of transactional identity and registered digital identity, as two sets of digitally stored information, the relationship of which is defined so that transactional identity connects digital identity with a physical individual (virtually represented through digital identity) through registered digital identity.

The purpose of identification is to establish identity for transaction purposes. Unlike transactions that take place on the basis of traditional, paper, identity certificates, where the individual is personally the actor of the transaction (physically present), in the case of digital transactions, the individual is not at the center, but the DI itself, or rather the transactional identity as its segment, plays a key role (Sullivan, 2014, p. 73). In this sense, transactional identity is more than just information, it enables a transaction to take place and is a gateway to further information about an individual. DI is the direct actor of the transaction, which takes place between two machines, through matching sets of information and data.

In the context of digital identity, we distinguish between authentication and identity verification. Authentication means an action that is performed on the basis of entering information during registration, i.e. after authentication, the identity is recorded or entered into the system. Verification is a process that is carried out at the level of transactional identity, that is, transactional identity is verified when the presented or entered information matches the registered information (matching information to information). Only then, on the basis of the verified transactional identity, transactions for the purpose of legal

traffic in the digital space can be verified. As a novelty, a legal presumption is introduced that the transactional identity is used only by the person whose data is stored within the registered identity, but the system cannot ensure this as absolute, so the presumption is rebuttable for the purposes of proving possible abuses.

At the moment when a transaction takes place, the identity is verified when all the displayed information from the domain of the transactional identity whose entry, or other form of presentation of the request, matches, i.e. when the matching is confirmed, with the information contained in the identity register that was created during the identity registration. In this sense, the identity is verified not by matching to the human being, or legal person, in question, but by matching the information presented at the time of the transaction with the information entered at the time of registration (Immorlica, Jackson & Weyl, 2019). For this reason, the transactional identity is often defined as a "token" identity (token identity), since at the time of the transaction, the identity is a token, i.e. sign, symbol, proof of identity. Therefore, we can make a distinction between traditional and transactional identity. Traditional identification documents, such as passports, are submitted in person when determining identity, i.e. a person is physically present for the purpose of establishing his identity, and the decision of the authorized person who determines the identity is based on his personal discretion. On the other hand, transactional identity is based on stored information about a person, and information are the subject of matching. And that information is not only for the needs of identifying a person, as in the case of traditional identification documents, but furthermore for the interaction of the system with the registered identity, and ultimately the transaction itself based on them.

The question can be raised as to who is the person with legal personality in the transaction that takes place on the basis of confirmation of the transactional identity, i.e. who is the entity entering into the legal relationship. Is it the person whose data was entered during registration or the person who enters the data of the transaction identity, because it does not have to be the same person, although most often it is? Is the transaction identity itself, as a set of information, a legal entity? Transactional identity is an abstract and artificial creation, and a human being is linked to a registered, or transactional, identity through a signature or biometric data, and it is used for remote transactions, which take place without personal contact of the participants (Sullivan & Stalla-Bourdillon, 2015, pp. 6–8). Therefore, such circumstances indicate that legal capacity and capacity for judgment are not part of the information in the scope of transactional identity, because they do not affect transactional

identity (if it is a minor, it would be obvious from the date of birth, as well as in the case of persons who are marked in the system as persons deprived of legal capacity). Transactional identity exists only as an abstract idea to function within legal transactions because law itself benefits from such a concept. For the existence of a legal subject, i.e. the treatment of any entity as a legal subject, it is sufficient for the legislator to decide in that direction, i.e. to grant the status of a legal subject by legal rules. In that case, the legislator only follows changes in business and legal practice.

In electronic transactions, proof of identity implies identity verification in two steps: first, some of the information that makes up the transactional identity is presented in order to establish the identity, and then, in the second step, the presented information is compared with the information stored or recorded in the register (chip on the ID card, or online register). After completing the two described steps, we can say that the transactional identity has acquired legal subjectivity. Here's why. Legal relations are established between the registered identity (through the transactional identity) and a public or private entity, as another participant in the transaction. The rights and obligations that arise on the basis of the completed transaction are first of all related to the transaction identity, and then to the registered identity, and not necessarily to the individual who is connected to the registered identity, i.e. the individual whose data constitutes the registered identity, nor with the individual who represents or enters the data that constitutes the transactional identity. Therefore, if we look at a contract that can be created electronically, the contract is concluded with a registered identity. Therefore, we can say that identity in the context of modern digital transactions consists of digitally stored information that is authentic and to which the law has assigned legal subjectivity (Sullivan, 2009, pp. 232–234).

Manufacturers and other stakeholders in modern, data-driven and digital, economy collect and refine raw personal data collected via their devices and capitalize on the resulting information assets. Regular users are usually completely unaware of the monetary value of their personal data and tend to underestimate their economic power within the data-driven economy and to passively succumb to the propertization of their digital identity. Academics and policy makers are increasingly aware of how data mining creates new privacy risks through identification and re-identification, therefore it is their job to introduce these risks to public (Beduschi, 2019). Personal data of individuals represent monetary value in the data-driven economy and are often considered a counter performance for "free" digital services or for discounts for online products and services, customer data and profiling algorithms are considered

a business asset. At the same time, individuals do not seem to be fully aware of. From the aspect of legal treatment of possible abuses of digital identities themselves, or individual data that make up a digital identity, it is possible to imagine the fraudulent use of someone else's transactional identity, that is, the data that make it up. In that case, the individual can prove an objective impossibility that he personally presented his transactional identity, that is, the information that constitutes it. In that context, it is necessary to create certain legal assumptions in law for such situations, but at the same time this does not dispute the fact that the contract or other legal relationship was created with a registered identity as the other party, even though it could be proven as flawed or destructible from the aspect of potential fraud.

In the context of the protection of human rights, we are talking about the right to identity, consequently related to the inadequacy of the application of the right to privacy in the context of DI, because transactional identity is precisely based on information that is largely public. It is debatable to what extent information about a personal name, date of birth or death, picture, and even a signature can be subject to privacy protection. What is the difference between the right to privacy and the right to identity? The right to privacy implies an individual's control over the collection, publication and use of his personal data (Goodell & Aste, 2019, pp. 16–18). The theoretical concept of the right to identity implies autonomy in the sense of recognition and recognition and treatment as a unique individual. In relation to the public interest, privacy has its limits, while identity should not legitimately be unilaterally taken away, changed or conditioned for reasons of public interest. The right to identity is threatened by false or untrue indications of identity, while the right to privacy is threatened by restrictions and interference with individuals' control over the collection, disclosure or use of personal information. The privacy of an individual can be limited in the public interest, i.e. it can be subordinated to it (for example in the case of security risks), while the right to identity cannot be subordinated to the public interest.

4. Concluding remarks - digital identity as determinant of the development of digital society

Digital identity as a modern form of human identity is primarily machine related. Telephone numbers, e-mail inboxes, or Internet Protocol (IP)-addresses, as digital aspects of identity, today gain importance with the omnipresence of digital space as a prime area for transactions. Today, routine transactions take

place almost entirely through computer technology, which is an integral part of trade and other transactions. The system recognizes the transactional identity and enters into legal interaction with the registered identity, and not with the individual as a physical entity. The individual whose data constitutes the registered identity is represented in the transaction through the registered identity, as a set of digitally stored information, which is the other side of the legal relationship. This is a common consumer transaction scheme today. Transactional identity determines the right of a natural person to be recognized as an individual, that is, the subject of a transaction, and to enter into a legal relationship, that is, a transaction (Balani, 2024, pp. 3–4). This implies the assumption that the person who possesses transactional identity information is indeed the person whose data constitutes the registered identity and that it is he who performs the transaction, that is, that person enters into a contractual relationship. Precisely in the systems that are based on the communication of transactional identities, the largest segment of trust is invested in an automated process, with minimal or even no influence of the human factor. In a system created in this way, digital information is the key player, not a human being. It is the computer, automated process or algorithm that performs intelligent functions and makes decisions, which cannot be implemented by human operational action.

In May 2024, the European Union adopted an updated version of the eRegulation (EU) No. 910/2014 (e-IDAS), known as eIDAS 2.0. The aim of the new version is to establish a European framework for digital identity, while also enabling the free use of qualified electronic signatures for citizens for non-professional purposes, as well as at the same time providing for the necessary measures to prevent natural persons from using qualified electronic signatures for professional purposes free of charge. In addition, eIDAS 2.0 introduces a number of new provisions relating to electronic identification, electronic signatures and the general security of digital transactions. The establishment of a European framework for digital identity is aimed at enabling a secure and interoperable digital identity for access to public and private services, both online and offline. This framework also introduces the European Digital Identity Wallet with the aim to enable citizens and businesses to securely store and share digital documents and digital identification data, as well as to sign documents using a qualified electronic signature. This scheme also includes the introduction of a digital identity cards, which would allow citizens to securely store and share their data, as well as to use a qualified electronic signature.

The digital society has brought new forms of communication, and what we call digital identity today appears on two tracks - in private digital interactions of individuals and legal entities for the purposes of advertising,

social networks, informal communication, etc (Gstrein & Kochenov, 2020). Every individual who once acted within the digital space has left a digital footprint on the basis of which they can be identified. The structure of information that constitutes a digital identity for these needs is determined by the parameters and rules set by the platforms that enable communication or other types of interaction in the digital space. On the other hand, the state moves its services into the digital space, requiring citizens to create a digital identity for the needs of accessing and using those services. More and more state services are provided via the Internet, which led to the creation of the concept of "digital citizenship" (Sullivan, 2014, p. 76). Following the example of traditional social theories, the concept of a digital social contract is discussed, precisely with the aim of achieving the integrity of the digital identity. This implies a joint venture of citizens, business entities and the state in creating a joint model of responsible digital citizenship. Regardless of whether the digital identity occurs in the context of private communication or government services, the same requirement for ensuring its integrity and security is the same. Also, regardless of the context in which DI occurs, it has significant personal, commercial and legal segments.

With the emergence of different forms of digital identities, both for individuals and legal entities, emerges a new concept of the so-called digital citizenship. Digital citizenship, which implies a certain degree of responsibility, i.e. the only model that is sustainable is the model of responsible digital citizenship, which is based on a digital social contract. Understanding the digital social contract rests on the rights, obligations and responsibilities that are distributed between individuals and entities that provide different services in the digital space. Rights, obligations and responsibilities are defined by various internal acts that regulate business in the digital space, as well as by public law regulations of national and supranational origin (such as data protection, choice of governing law, license validity, etc.). The development of digital identities, and the creation of a new category of digital citizenship, is part of the world's digital future.

ACKNOWLEDGEMENT

The paper is the result of a long-term scientific research project, *Progressive Development of Law in the Modern Digital Society*, financed by the Provincial Secretariat for Higher Education and Scientific Research (Decision No. 003069523 2024 09418 003 000 000 001-01003069523 2024 09418 003 000 000 001-01, 21 November 2024).

Conflict of Interest

The authors declare no conflict of interest.

Author Contributions

Writing - original draft, P.M.; Writing - review and editing, J.S.D. and resources, N.A.O. All authors have read and agreed to the published version of the manuscript.

Mirković Predrag
Univerzitet Privredna akademija u Novom Sadu, Pravni fakultet za privredu i pravosuđe u Novom Sadu, Novi Sad, Srbija

Stojšić Dabetić Jelena
Univerzitet Privredna akademija u Novom Sadu, Pravni fakultet za privredu i pravosuđe u Novom Sadu, Novi Sad, Srbija

Aleksić Oliveira Nina
Univerzitet Privredna akademija u Novom Sadu, Pravni fakultet za privredu i pravosuđe u Novom Sadu, Novi Sad, Srbija

DIGITALNI IDENTITET KAO NOV PRAVNI KONCEPT

APSTRAKT: Sa razvojem savremenog digitalnog društva povećava se stepen interakcije subjekata koja se odvija u digitalnom prostoru, a sama interakcija se zasniva na korišćenju ličnih podataka između subjekata, u cilju potvrđivanja i verifikacije njihovog identiteta. Pitanje primene ličnog identiteta u digitalnom prostoru stvorilo je realnost *de facto* postojanja digitalnog identiteta kao novog oblika lične identifikacije. Digitalni identitet je identitet koji se sastoji od informacija koje se čuvaju i prenose u digitalnom obliku. Dakle, postavlja se pitanje kako se novi koncept ličnog identiteta kao digitalnog identiteta može obuhvatiti pravnim pravilima, da bi se omogućile transakcije. Autori tvrde da digitalna tehnologija

poziva na novu filozofiju identiteta. Takođe tvrdimo da digitalni identitet nužno iziskuje redefinisanje tradicionalnog pravnog okvira. U nastavku rasprave u ovom radu videćemo ko se može tretirati kao pravni subjekt u transakcijama koje se sprovode putem digitalnog identiteta. Razmotriće se i pitanje kako se zakonske pretpostavke mogu promeniti da bi uključile nove realnosti, a kao najvažniji deo, predstavićemo pravni tretman tehničke strukture od koje se sastoji digitalni identitet.

Ključne reči: *digitalni identitet, transakcioni identitet, lični podaci, pravne transakcije, registrovan identitet, digitalno građanstvo*.

References

1. Balani, H. (2024). *Securing the Future of the EU Digital Identity Wallet: Why we need Corporate Digital Identity standards now.* Downloaded 2024, July 30 from https://ssrn.com/abstract=4910859. DOI: http://dx.doi.org/10.2139/ssrn.4910859
2. Beduschi, A. (2019). Digital identity: Contemporary challenges for data protection, privacy and non-discrimination rights. *Big Data & Society*, pp. 1-6. DOI: 10.1177/2053951719855091
3. Bwana, R. O. (2024). Kenya's Digital Identity Revolution: Balancing Progress and Human Rights. *Global Privacy Law Review*, *5*(2), pp. 82–87
4. Dash, B. & Sharma, P. (2021). Digital Identity and Authentication in the Blockchain Era. Downloaded 2021, January 28 from https://ssrn.com/abstract=4567733. DOI: http://dx.doi.org/10.2139/ssrn.4567733
5. Finck, M. (2018). Blockchains and Data Protection in the European Union. *European Data Protection Law Review*, *4*(1), pp. 17–35
6. Gstrein, O. J., & Kochenov, D. (2020). Digital Identity and Distributed Ledger Technology: Paving the Way to a Neo-Feudal Brave New World?, *Frontiers in Blockchain, 3*(10), pp. 1–8, DOI: doi.org/10.3389/fbloc.2020.00010
7. Goodell, G., & Aste, T. (2019). A Decentralised Digital Identity Architecture, *Frontiers in Blockchain*. Downloaded 2025, January 15 from https://ssrn.com/abstract=3342238, DOI: doi:10.3389/fbloc.2019.00017
8. Immorlica, N., Jackson, M., & Weyl, E. (2019). Verifying Identity as a Social Intersection, *SSRN Electronic Journal*. Downloaded 2025, January 15 from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3375436. DOI: http://dx.doi.org/10.2139/ssrn.3375436

9. 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 – e-IDAS
10. Sullivan, C. (2009). Digital Identity - The Legal Person?, *Computer Law & Security Review, 25*(3), pp. 227–236. DOI: https://doi.org/10.1016/j.clsr.2009.03.009
11. Sullivan, C. (2013). Is Your Digital Identity Property? An Examination of Digital Identity in the Era of e-Government and Digital Citizenship, *European Property Law Journal*, *2*(2), pp. 122–143. DOI: 10.1515/eplj-2013-0010
12. Sullivan, C. (2014). Digital citizenship and the Right to Digital Identity under International Law. In: Kierkegaard, S. (ed.), *Information Ethics and Security – Future of International World Time* (pp. 72–84). Paris: International Association of IT Lawyers. Downloaded 2025, January 15 from https://ssrn.com/abstract=2519806
13. Sullivan, C., & Stalla-Bourdillon, S. (2015). Digital Identity and French Personality Rights – A Way Forward in Recognizing and Protecting an Individual's Rights in His/Her Digital Identity. *Computer Law & Security Review*. Downloaded 2025, January 15 from https://ssrn.com/abstract=2584427
14. Wang, F., & De Filippi, P. (2020). Self-Sovereign Identity in a Globalized World: Credentials-Based Identity Systems as a Driver for Economic Inclusion, Self-Sovereign Identity in a Globalized World: Credentials - Based Identity Systems as a Driver for Economic Inclusion. *Frontiers in Blockchain*, Special Issue on Identity and Privacy Governance. Downloaded 2025, January 15 from https://ssrn.com/abstract=3524367
15. Zwitter, A., Gstrein, O., & Yap, E. (2020). Digital Identity and the Blockchain: Universal Identity Management and the Concept of the „Self-Sovereign" Individual. *Frontiers in Blockchain*, *3*(26), pp. 1–14. DOI: https://doi.org/10.3389/fbloc.2020.00026