MetaverseUA Chair

Academic Chair for the Responsible Development of the Metaverse

A unique digital identity in the metaverse: state of the art and future challenges

Proceedings of the International Congress Towards a Responsible Development of the Metaverse, 13-14 June 2024, Alicante

Giovanni Sorrentino

University of Bologna

catedrametaverso.ua.es

Universitat d'Alacant
Universidad de Alicante

The Chair for the Responsible Development of the Metaverse (MetaverseUA Chair) was created by the University of Alicante (Spain) and financed by Meta Platforms under its XR Program and Research Funds. The Program aims at supporting academic and independent research across Europe into metaverse issues and opportunities. The MetaverseUA Chair is a member of the European Metaverse Research Network. Like all our work, this report has been produced completely independently. The ideas expressed in this paper are the sole responsibility of the author.

How to cite this paper:

Sorrentino, G., 'A unique digital identity in the metaverse: state of the art and future challenges´ (2024) *Proceedings of the International Congress Towards a Responsible Development of the Metaverse, Alicante, 13-14 June, 2024.*

Abstract

“On the Internet nobody knows you are a dog”. This was the slogan that characterised users' use of the Internet for years. As a result, each user was (and is) allowed to possess many different digital identities, often unrelated to each other, and bearing no resemblance to the person’s real identity. The start of the Web 4.0 era and the advent of the Metaverse, however, pose many challenges to the protection of individual rights. One of the most important challenges concerns digital identity. While it is important to ensure maximum freedom, users increasingly demand 'authenticity'. Moreover, this fragmented nature does not allow for adequate identity protection and is an obstacle to interoperability, a much-desired feature of the metaverse. This article aims to examine the state-of-the-art of the Metaverse, with a focus on issues related to digital identity. After introducing the concept of digital identity, the article analyses the effectiveness of the current European regulatory framework, and end by discussing the possible benefits of a single digital identity.

Keywords: Digital Identity, Metaverse, Identification, eIDAS, Law

Table of contents

1. Introduction

The sentence "On the Internet, nobody knows you are a dog" epitomized the anonymity that characterized the early days of internet usage. Users could have multiple digital identities, often unrelated to each other and to their real-world personas. However, the transition to Web 4.0 and the emergence of the Metaverse bring new challenges to the protection of individual rights, particularly concerning digital identity. In this evolving digital landscape, users seek both greater authenticity and freedom, but the fragmented nature of current digital identities hampers both adequate protection and the benefits that the Metaverse's interoperability provides.

This article explores the state of the art of digital identity, specifically focusing on the Metaverse and digital identity issues. This analysis highlights the importance of a cohesive and secure digital identity framework to enhance user trust and authenticity, facilitate interoperability, and promote seamless interaction within the Metaverse.

In the context of the Metaverse, digital identity encompasses all characteristics and elements that allow a person to be recognized within this virtual environment. The digital world presents numerous risks, including identity theft, misuse of personal data, and difficulties in managing multiple digital personas. Ensuring the integrity and protection of digital identities is crucial as interactions and transactions become more complex and diverse in this virtual space.

The article further delves into the legal aspects of digital identity, discussing the implications of various regulatory frameworks across different countries. By comparing the approaches of the EU, UK, Australia, and the USA, this paper aims to provide a comprehensive understanding of the global landscape of digital identity regulation and its impact on the future development of the Metaverse.

2. What is (digital) identity?

The answer to the question "Who am I?" can vary greatly depending on the context and the individual being asked. One might respond with their given name, a nickname, or describe a personal characteristic. They might also elaborate with details of their occupation, hobbies, or physical and personality traits. A photo might also serve as an answer. Responses change depending on one's environment too. In an office setting, one might include their place of work and job title, while in a more casual setting, they might mention their name and place of origin. Indeed, all these answers are correct because they all say something about who you are. In other words, they are saying something about your identity.

Identity has traditionally been a nebulous notion and in referring to 'identity' without defining it, much of the legal literature in this area lacks precision. This lack of rigour gives the impression that 'identity is identity' whereas the constitution, function, and nature of identity depends on its context.[1]Identity is what defines someone and distinguishes them from another person. In the field of psychology, the scientific study of the mind and behaviour, identity is defined by the qualities, beliefs, and personality of a person. In the

[1] C Sullivan, Digital Identity: An Emergent Legal Concept (2011), University of Adelaide Press. https://www.jstor.org/stable/10.20851/j.ctt1sq5wqb

closely related field of sociology, the scientific study of society, we get a slightly different definition, which takes into account culture, history, and religion.[2]

The concept of identity is vast and encompasses many different notions. Therefore, despite various efforts, a complete and exhaustive definition of identity has never been agreed upon. However, the core of identity is formed by essential elements required for the identification of a person. Primarily, these are names and images. A name, consisting of first and last name, serves the social function of identifying a person within society. The importance of a name within society is demonstrated by the fact that, in most legal systems, one cannot be deprived of their name.[3]

In other words, "identity" is not solely one's name and surname. The concept of identity encompasses all the characteristics and elements that allow a subject to be recognized by society. The concept includes both tangible elements (such as our appearance), as well as intangible ones (e.g. ideas).

Furthermore, identity consists of layered aspects of cultural heritage, ethnicity, age, professional and social roles, hobbies, gender identification, sexual orientation, and much more. These elements of identity can be sources of pride and self-expression. Name and image are not the only elements used to identify a person. Other data related to or connected with a person may also facilitate identification, especially following technological developments. For instance, one could consider voice, fingerprints, biometric data, digital signature, username, or electronic identification data, matriculation numbers, and codes assigned by public administrations (tax code, health code, etc.) as identifying elements as they allow for the unequivocal identification of a person.[4] Image, on the other hand, is an innate means of identification, describing a person's features in a way that makes them recognizable. Representation is closely related to image; it is defined as the means by which an image circulates in society.

From a legal point of view, the term human identity should be understood as a relatively new human right which was initially derived from the interpretation of Article 8(1) of the ECHR: "Everyone has the right to respect for his private and family life, his home and his correspondence." However, identity as a human right had already established itself in the area of international law and had also already been accepted into the canon of European Union regulations (see the introduction of the Charter of Fundamental Rights of the European Union), meaning it can be considered a universal law. From a jurisprudential point of view, the right to identity has not yet been comprehensively addressed in a single ruling of the European Court of Human Rights, but its various elements can be interpreted from a combination of judgments. First of all, we can assume that the right to identity protects elements of identity such as name, surname, right to know one's origin, gender, and ethnicity[5]. However, it should be noted that this catalogue of elements is only one example. Over the years, the content of the right to identity has been expanded with elements such as image, citizenship (Relu Adrian Coman and Others v Inspectoratul General pentru Imigrări and Ministerul Afacerilor Internet, 2018), voice, and pseudonym being added and protected by human rights law. Moreover, it is worth noting that the

[2] Doerk A, 'An introduction to self-sovereign identity (SSI)' (2019) https://ssi-ambassador.medium.com/an-introduction-to-self-sovereign-identity-ssi-916eb42f0490.

[3] World Economic Forum, 'Metaverse Identity: Defining the Self in a Blended Reality' (Insight Report, March 2024).

[4] G Resta, 'Identità personale e identità digitale' (2007) Dir Informatica 511.

[5] Cfr. Odièvre v. France, Application no. 42326/98 (European Court of Human Rights February 13, 2003). Mikulić v. Croatia, Application no. 53176/99 (European Court of Human Rights February 7, 2002). http://www.aimjf.org/storage/www.aimjf.org/Jurisprudence_CEDU/CASE_OF_MIKULIC_v._CROATIA.pdf. Godelli v. Italy, Application no. 33783/09 (European Court of Human Rights September 25, 2012).

content of the right to identity is constantly evolving, and thus new elements of human identity are being incorporated into the protection of this right, e.g. freedom of dress, sexual identity, and internet identity.[6]

In summary, personal identity describes the entirety of personality that distinguishes an individual from all others. Therefore, constituent elements are those that allow the differentiation of a person within a community. Among these, the following stand out in particular: natural entity (name, surname, birth, etc.); and legal entity (legal roles, attestation, and credentials).

In the past decades, the internet has significantly changed the way we live, shaping a new world with rules that differ slightly from those of the past. In this new context, some rights have had their scope expanded, while others have become subject to risks that did not previously exist in the "real" world. This is the case with the right to privacy, for example, but it is also true for the right to identity.

In the case of privacy, legislators (especially but not only in Europe) have been proactive in enacting protective legislation. However, this has not been the case for identity. Identity has changed its nature, reaching a new and broader dimension, and while in the real world, the individual is in total control of their identity, this is not always the case in a digital context. Identity theft can serve as a valid example. Furthermore, in the real world, identity is substantially reduced to just a name, demographic data, and image, while in the digital environment, other concepts such as avatars and digital twins gain importance. In the digital world, identity is subject to many more risks compared to the physical world.

Nonetheless, the right to identity, despite being affected by the changes that have taken place in the world over the last decade, has not received the necessary attention from neither legislators nor legal scholars. For these reasons, we can say that the concept of identity is a new one and is gaining importance due to the changes brought about by the development of the digital world. So now, in a world that is strongly impacted by changes brought on by technology, identity (particularly digital identity) is becoming not just important but crucial. Interactions and transactions become more complex and diverse, in the digital environment. For this reason, it is necessary to think about an adaptable identity framework as a bedrock upon which digital trust, authenticity, and digital experiences can be built.[7] In such context (i.e. the metaverse), the identity is founded by two main pillars:

- Human→ e.g. an individual's identity; this may be manifested through a digital entity
- Digital Entity → e.g. avatars, chatbots, virtual agents, digital twins, etc.

In an era in which our online identity is central to accessing information and services, ensuring the integrity of that identity is increasingly important. It is clear that whatever technology we use as a basic framework for this purpose needs to be flexible enough to display an incredible amount of human diversity and to guarantee users' right to identity[8].

[6] E. Michalkiewicz-Kądziela and E. Milczarek, 'Legal Boundaries of Digital Identity Creation' (2022) 11(1) Internet Policy Review 113.

[7] World Economic Forum, 'Metaverse Identity: Defining the Self in a Blended Reality' (Insight Report, March 2024).

[8] A Doerk, 'An introduction to self-sovereign identity (SSI)' https://ssi-ambassador.medium.com/an-introduction-to-self-sovereign-identity-ssi-916eb42f0490 accessed 27 May 2024.

3. Difference between Digital Identity and Identification

What unites the identities that can be created in various digital worlds is always the physical person behind them. The process that allows for the verification of that physical person is identification. The concept of identity differs significantly from the concept of identification. The latter refers to the process of verifying that the declared identity matches the actual identity. While the two concepts are often confused, it is essential to distinguish between them.

Digital identity is the information required to establish an individual's identity for official purposes, to access and use public sector services. It is, as previously described, the collection or set of identity information that is typically full name, gender, date of birth, and identifying information, such as a unique number, signature, or biometric that links to a person (Sullivan, 2023).

Identification is a better term to describe a proof, a system, or a transaction involving a subject and an evaluator, centred around verifying a claim of identity (i.e. that a person is one person and not any other). It also applies to the recording of certain attributes — biodata, biometrics, claims — in a formal record, a "credential," that grants specific rights or permissions to the individual. Identification is a concept we care about because it is that process that grants access and rights; it is the representation of the individual within and to an administrative system.[9]

Identification is just one part of the two processes used to establish identity for a transaction. Although in some respects, transaction identity may seem to replicate the traditional function of identity credentials such as identity papers and even a passport, there is an important distinction. Unlike traditional identity papers, the information that comprises transaction identity plays a critical role in the transaction, not the individual.[10]

Managing digital identities may involve the intricate processes of creating, maintaining, and using a combination of credentials and assets across platforms – potentially in a digital wallet. It is possible that in the future a user's digital identity will not be a single entity, but rather a unique core linked to a myriad of other digital entities, resulting in a web of highly complex and interconnected information strands. Ownership and control will influence the management of identities, while ethical considerations should guide how identities are used, shared, and represented.

4. State of the art

Digital identity can be understood as the representation of oneself within a virtual environment. This representation includes numerous elements that refer to our being. Our name, our image, our contact information. But also, our statements and our ideas. Within the metaverse, all these elements are potentially even more at risk. There has never been a "place" until now capable of collecting so much data, and because the metaverse has increasingly become a place where users live part of their lives (acting, performing actions, and interacting with other users), there exists unprecedented exposure of an individual's identity. Until now, we have been accustomed to treating identity as a single concept. In

[9] Whitley, E. A., Gal, U., & Kjaergaard, A. (2014). Who do you think you are? A review of the complex interplay between information systems, identification and identity. European Journal of Information Systems, 23(1), 17–35. https://doi.org/10.1057/ejis.2013.34.

[10] C Sullivan, 'Digital identity – The legal person?' (2009) 25(3) Computer Law & Security Review 227.

the "real" world (or rather, offline), people generally have a single identity, and modifying it or creating "alter egos" is often difficult or physically impossible.

The phenomenon of multiple identities has emerged in a meaningful way, in part, due to the advent of social networks. Some users of these networks began creating multiple profiles, using pseudonyms or even fake names. The secondary profiles were often "fake" and revealed an identity that did not correspond to the true one. Many of these secondary profiles also used fake images, invented names, or even the identities of others. Various social networks were therefore limited in this regard: the control over one's data was much simpler, as users only exposed the information they wanted to reveal. For example, users could publish a certain profile image instead of another and choose to publish personal posts as they saw fit. Many social networking sites invoke a ‘real names’ policy and disallow the creation of multiple accounts by a single individual.[11] However, this is not always sufficient to ensure that the user provided data corresponds to reality. The metaverse offers many more possibilities for personalization and control over one's virtual character and enables a much more complete interaction between users. However, in this virtual world, much more data is exposed. Indeed, here the user can create multiple identities, all of which are at least partially or entirely corresponding to the real identity. Of course, there is the possibility that the created profile has no true reference in real life, but often the opposite occurs. The user creates an avatar, which becomes a true alter ego. The user is reflected in their avatar, which acts as a true "digital twin". In addition, a user can create multiple avatars, each of which potentially revealing something real about the identity of the user or simply be part of their own virtual identity.

Furthermore, in the digital world, each of us uses numerous websites and platforms. Many of these require registration so that the user's identity can be stored, recognized and identified on subsequent access. The enactment of online identity and management of multiple identities across different online domains create by their very existence issues of identification. In most cases, identification is managed through the combination of username and password.

Currently, the primary techniques used for identification, or rather authentication, are based on information that distinguishes the author. This distinguishing information can fall into one of three categories: something you know, something you are, or something you have. The first, and most widespread, method of authentication in the field of electronic signatures, is the association of username and password. The user distinguishes themselves from others by something they know. Authentication is therefore based on the agreement between the current user input and previously saved information, which only the user should know. This system offers some advantages, including relatively low management costs and ease of use for users. However, it is a relatively insecure and unreliable system. In fact, it does not guarantee that the person inputting the credentials is actually the person to whom those data belong. Nothing prevents passwords from being revealed to a third party or, worse, stolen. Password thefts are extremely common and virtually impossible to prevent.

Another mechanism of identification can be related to the concept of "something you have". In this case, the association is made between a code, or a username, and a device uniquely assigned to the individual. This can be a smart card, a USB key, or a token (i.e., a physical device used to obtain a secret temporary code) or, as is often the case, a

[11] O Tene, 'Me, Myself and I: Aggregated and Disaggregated Identities on Social Networking Services' (2012) Journal of International Commercial Law and Technology, SSRN https://ssrn.com/abstract=1959792 accessed 27 May 2024.

smartphone. This is a much safer system than single-factor authentication, and for this reason, it is often used in banking operations. However, even with this method, there are risks: the code could be intercepted, or the device could be lost. Recently, two-factor authentication has been performed through the sending of a code to a mobile device. Although it is a step forward in terms of security, this system is not able to guarantee that the user accessing it is actually who they claim to be. It only ensures that they possess the associated security device.

In the case of authentication through the "something you are" system, biometric techniques are used, i.e., through the recognition of innate physical or behavioural characteristics of the person. Among these techniques, the most well-known are facial recognition, retinal analysis, fingerprint analysis, hand geometry, voice verification, and DNA analysis. These techniques certainly provide a higher level of security in recognizing the real user. However, the risks are significant. This is not because the data are easily compromised, but because if the biometric data are actually compromised or stolen, the risks are extremely high. For example, in the case of a stolen password, the user can reset it or create a new one. Biometric data, on the other hand, are by their nature immutable or nearly so. Should these data be stolen, therefore, it would open the enormous problem of *real* (or, more accurately, *offline*) identity theft, with incalculable damage to the victim. Furthermore, it is worth considering that biometric data are the most sensitive category of data and for this reason, their treatment is prohibited, in the EU, by various regulations, including Regulation 2016/679 (GDPR) and AI Act.

The importance of this topic can be easily understood if we consider the value of identity theft in the USA in recent years. According to an Exploding Topics's report, 87% of people leave personal information exposed online. In total, 9 in 10 people allow personal information to be exposed online while doing activities such as using email services or accessing bank accounts. Furthermore, almost one-third of Americans have been a victim of identity theft during 2023. The Federal Trade Commission in the US received 5.7 million total fraud and identity theft reports, 1.4 million of which were identity theft cases, with an estimated total loss of around $10.2 billion in 2021. In recent years, these numbers have increased with total losses of $43 Billion in 2023.[12]

Typically, identity is managed one application at a time. This means that individuals are asked to maintain dozens of different usernames and passwords, one pair for each website with which they interact. The complexity of this current system is a burden for both individuals and businesses. Individuals are driven to reuse passwords or utilize trivial ones such as relatives' birthdates, making online fraud and identity theft easier. Businesses, on the other hand, are required to manage the identity of users despite not often having the resources or interest to do so.[13] This problem is even more evident and invasive in the metaverse(s) where users are forced to use a different identification system for each virtual world, and compelled to hold different identification keys, thus preventing them from operating between different worlds quickly.

Furthermore, the importation of tokens from one world to another is prevented, forcing the creation of as many different identities as there are platforms in which the user acts. All of this results in serious information security problems. Managing multiple profiles

[12] Federal Trade Commission, Consumer Sentinel Network Data Book 2022 https://www.ftc.gov/reports/consumer-sentinel-network-data-book-2021 accessed 27 May 2024.

[13] O Tene, 'Me, Myself and I: Aggregated and Disaggregated Identities on Social Networking Services' (2012) Journal of International Commercial Law and Technology, SSRN https://ssrn.com/abstract=1959792 accessed 27 May 2024.

and different identification systems exponentially increases the likelihood of being the target of cyber-attacks and identity theft. In addition, the quality of the user experience is reduced as is the potential of the metaverse. For this reason, one of the most important challenges that metaverse platforms must face is related to interoperability.

Interoperability is defined as the ability to interact with, exchange, and make use of data and resulting information to enable movement, transactions, and participation across systems, platforms, environments, and technologies. Digital identity is the nexus to an interoperable metaverse. It enables accountability and the capacity to traverse worlds with minimal friction. Identity is also highly contextual. For example, a punk rocker may want to disassociate from their musical persona during their workday as an attorney. Where possible, interoperability should honour the human-first need for selective anonymity and pseudonymity to protect user privacy while respecting the tension between self-expression and creating safe environments.[14]

5. Legal Frameworks

In a context where identity is becoming increasingly significant, many countries have recognized these issues and the necessity of regulating this matter promptly. Consequently, several legislators have begun to pay attention to this topic, leading to the first regulations in the field. As the solutions set forth by each country can vary, a reflection on each approach could be beneficial in understanding how different legal systems are acting concerning this topic

Throughout the world, 81 countries have a digital identity (eco)system that enables fully remote authentication for online transactions. This includes 74 countries with a national ID system and 7 countries without one. Most countries with online digital identity solutions—51 out of the 81—are high-income countries and another 20 are upper-middle income countries. From a regional perspective, online digital identity solutions are most prevalent in Europe, the Middle East, Latin America, and East Asia.[15]

It is also important to understand how different countries are currently managing the topic. The following will analyse the main features of the laws and policies adopted by the EU, USA, Australia, and the UK.

In Europe, Belgium was the first country to issue 'smart' identity cards. The eID scheme was rolled out in 2003 and individuals in Belgium now use their identity card to transact with government entities for transactions ranging from filing taxes and applying for official documents such as a marriage certificate to accessing public libraries and sporting facilities. Even more significantly, the private sector uses the eID card infrastructure for commercial transactions. After Belgium, other European countries have started drafting legislation on identity as well.

In Estonia, where digital ID and online authentication have been used for two decades, 98 percent of the population is believed to use their credentials regularly to

[14] World Economic Forum, 'Metaverse Identity: Defining the Self in a Blended Reality' (Insight Report, March 2024).

[15] A. Z. Metz, C.S.Casher and J. M. Clark, ID4D Global Dataset 2021: Volume 2 - Digital Identification Progress & Gaps (World Bank Group) http://documents.worldbank.org/curated/en/099020824141510923/P176341192f2c50e11bc5619be95c4fb2ed accessed 27 May 2024.

access more than 5,000 online services.[16] Launched in 2018, France's "FranceConnect" digital identity solution had 40 million users—about 70 percent of the adult population— and facilitated access to over 1,400 online services by 2022.[17]

Outside of Europe, Singapore's Singpass has more than 4.5 million users or about 97 percent of the adult population.[18] In Brazil, more than 150 million people have registered with gov.br, including 45 million high-assurance 'gold' accounts that allow for secure access to the widest online services and transactions.

At the moment, many of the countries globally have foundational ID systems that support some form of digital identity verification and/or authentication for in-person services and transactions. It means that the countries are increasingly moving forward with systems that support digital identity.

In recent years, for instance, issues in the European Union related to the digital world have become a priority. For this reason, the EU published the Regulation n. 910/2014 on electronic identification and trust services for electronic transactions (better known as e-IDAS Regulation). It was written to build trust in the online environment by providing a common legal basis for secure electronic interactions.[19] The initial objective of eIDAS 1.0 was to eliminate the differences between the identification systems of various countries, in order to promote interoperability and therefore facilitate the European single market. This was made clear by Article 1. This article set the purpose of ensuring the proper functioning of the internal market while aiming at an adequate security level of electronic identification means and trust services. One of the objectives of this regulation was to remove, between Member States, the existing barriers to the cross-border use of electronic identification means used to authenticate public services at a minimum (see whereas 12) to promote interoperability between EU countries. Furthermore, art. 3(1)(1) defined electronic identification as "the process of using person identification data in electronic form uniquely representing either a natural or legal person or a natural person representing a legal person", while Art. 3(1)(2) states that 'electronic identification means' is 'a material and/or immaterial unit containing person identification data and which is used for authentication for an online service'.[20] In addition, the regulation, in Article 8, establishes three levels of security: low, substantial and high, and sets forth the requirements that each of these levels of security must have. Another principle adopted by the legislator in the eIDAS regulation is technological neutrality. In order to establish a framework for interoperability, it is stipulated that there should be no discrimination between nationally regulated electronic identification solutions, as per each State's technical approaches.

Over time, the eIDAS regulation has been shown to have several limitations, and its goal has not been totally achieved. The utilization of digital identities under eIDAS 1.0 was very fragmented between the Member States. For example, additional attributes like diplomas, power of attorney, or also machine identities could not be utilized in a legally compliant manner within eIDAS 1.0. To overcome these issues, in June 2021, the European

[16] B. Oyetunde, 'The making of a giant: Estonia and its digital identity infrastructure' (2022) e-Estonia https://e-estonia.com/the-making-of-a-giant-estonia-and-its-digital-identity-infrastructure accessed 27 May 2024.

[17] République française, 'FranceConnect' https://franceconnect.gouv.fr/ accessed 27 May 2024.

[18] World Bank, National Digital Identity and Government Data Sharing in Singapore: A Case Study of Singpass and APEX (2022) accessed 27 May 2024.

[19] Zaccaria A., M Schmidt Kessel, R Schulze and A M Gambino, EU eIDAS Regulation – Article-by-Article Commentary (Beck Hart Nomos 2020).

[20] M Zichichi, C Bomprezzi, G Sorrentino and M Palmirani, 'Protecting digital identity in the Metaverse: the case of access to a cinema in Decentraland' in Proc of the 5th Distributed Ledger Technology Workshop (Bologna, Italy, 25-26 May 2023) 1.

Commission published a proposal on amending eIDAS 1.0 with the aim to establish a framework for a European Digital Identity or, in other words, eIDAS 2.0. The main goal of the proposed update was not to create a replacement but to further develop eIDAS 1.0 in the context of decentralization and the upcoming SSI-paradigm[21].

It has to be noted that eIDAS 2.0 will expand the scope of eIDAS 1.0 beyond just identification and authentication to include additional cross-border digital services such as device identification. The initiative also strives toward increasing security levels and privacy safeguards with regard to electronically stored identities, as well as creating the European digital identity framework for simpler and harmonized creation and use of digital identities. Furthermore, eIDAS 2.0 aims to facilitate public procurement processes and improve interoperability between different national systems. These advancements promise to bring more efficiency and reliability to online services provided by public bodies or businesses operating in multiple countries.

The biggest change in eIDAS 2.0 is the requirement for every member state to provide a Digital Identity Wallet (EUDIW) to its citizens. According to the European Commission, under the new Regulation, the EU Member States will offer citizens and businesses digital wallets that will be able to link their national digital identities with proof of other personal information (e.g. driving licence, diplomas, bank account). These wallets may be provided by public authorities or by private entities, provided they are recognised by a Member State. Since the passage of eIDAS 2.0, some countries have already started to launch their own digital identity wallet. Belgium, for example, has become one of the first countries to launch a digital identity wallet. The Belgium Federal Government promised that the app for digital identity "MyGov.be" will provide a smoother experience with administrative work. By 2025, the app will incorporate eIDs and mobile driving licenses and by 2026, the European Health Insurance Card will have been added.

The digital wallet enables users to securely store and manage their European digital identities, providing them with full and exclusive control over their data. This allows users to access services provided by public institutions across any Member State without the requirement of additional physical documentation. The EUDI wallet also encompasses attestations of attributes, ranging from ePassports and driver's licenses to university diplomas, as well as personal information such as medical records or banking details. Furthermore, the wallet grants users access to a diverse range of online private and public services and enables them to affix qualified electronic signatures and seals to documents.

Another important aspect of the new European Digital Identity Wallet is that it will enable all Europeans to access services online without having to use private identification methods or share personal data unnecessarily. With this solution, each user will have full control of the data they share.

The objective of the EU is to create an "identity single market". This would enable users to be more readily identified within the European area, particularly in the digital context. Furthermore, having a unified identification system would enhance the security of identification processes. When applied to the metaverse, this could be a step towards the interoperability that has been advocated for by users. However, there are numerous obstacles. Firstly, finding a balance between freedom and security remains challenging. Arguably, in the metaverse, unlike in the real world, a user could have a different avatar for each platform, with vastly different features. While it is necessary to ensure that the user

[21] I Alamillo and S Schwalm, 'The possible impacts of the eIDAS 2.0 digital identity approach in Germany and Europe' (2023) Open Identity Summit 2023 DOI: 10.18420/OID2023_09 (Gesellschaft für Informatik e.V., Bonn) 109.

has the freedom of self-representation, it is also essential to ensure an higher evel of security in identification. After all, identity is a fundamental concept particularly in terms of the validity of transactions, which could be compromised if the counterparty is not able to be precisely identified. In the metaverse, transactions are numerous and increasingly economically significant.

Moreover, it is important to consider that the metaverse has a global dimension, not just a European one. This means that the metaverse has immense potential, but also that a unified identification system like that proposed by eIDAS may not be sufficient. To ensure the effective usability of the metaverse, identification tools must necessarily be more ambitious. For instance, when a European user utilizes the EUDIW and an American user utilizes another identification system, this creates an imbalance, with negative consequences for the utilization of the metaverse.

To guarantee a very interoperable and safe system, it is necessary that the user is truly sovereign over his identity and the elements associated with it, without an intermediary or a provider in which to place trust. After all, identity is one of the most personal aspects of an individual because it is the sum of all of that person's characteristics. Entrusting the management of this information to a third party is a risk in itself. Furthermore, granting full sovereignty of this information to the owner of the information would facilitate interoperability between different countries and different platforms. However, despite the user keeping full control of their information, the choice between entrusting management to a private or a public provider still remains. In both cases, there could be concerns and drawbacks, with an equilibrium becoming increasingly difficult to find.

Given the increasing importance of digital identity, countries outside the EU, including the UK, Canada, and Australia, have moved to adopt regulations, policies, or standards to regulate this issue. The UK, for example, has launched a Digital Identity and Attributes Trust Framework focused on enabling standard-based digital identity solutions that can work across the public and private sectors. The UK Digital Identity and Attributes Trust Framework provides a baseline standard for the secure use of digital identities. This framework is aimed at the identification, attribution, and orchestration of service providers. In March 2023, the Data Protection and Digital Information (No.2) Bill had its first reading in Parliament. This regulation has been strongly influenced by the identity framework and is intended to be strongly related to it. The bill will underpin the trust framework and its governance and allow identity and eligibility checks to be made against trusted, government-held data. The UK's strategy is a good example of how digital identity and data protection should relate to and be in harmony with one another. Indeed, it is not possible to maintain a secure identity without secure data management, and personal data protection alone is not sufficient to ensure that of identity. In Europe, this should occur through the synergy between eIDAS and GDPR. However, the two regulations do not coordinate well with each other.

Understanding this, Canada opted to create a single comprehensive Pan-Canadian Trust Framework (developed jointly between the government and the private sector) to accelerate the use of privacy-preserving digital identity solutions. The Pan-Canadian Trust Framework (PCTF) is a risk mitigation framework comprising a set of rules, standards, specifications, regulations, and guidance that offers a high-quality and versatile defined-code-of-practice for operating trustworthy and efficient digital identity, credentials, and supporting services. Its main goal is to contribute to the trustworthiness and interoperability of public and private sector digital trust and identity capabilities while prioritizing user-centered design, privacy, security, and convenience.

Finally, Australia has created a National Strategy for Identity Resilience and is advancing legislation to accelerate the creation of state and territory-issued digital credentials. The Strategy consists of ten principles to guide identity resilience. It includes immediate, medium, and long-term initiatives that will strengthen identity security arrangements across jurisdictions and works in combination with the Trusted Digital Identity Framework (TDIF). It is an accreditation framework for digital ID services that sets out the requirements that applicants need to meet to achieve accreditation. The accreditation framework and process ensures all identity providers meet strict rules and standards for usability, accessibility, privacy protection, security, risk management and fraud control.

In this context, the choice of the USA to not adopt legislation concerning the regulation of digital identity is peculiar. The lack of an easy, secure, and reliable way for entities to verify the identities of people they are dealing with online creates friction in commerce, leads to increased fraud and theft, degrades privacy, and hinders access to many online services. While most countries are adopting regulations or policies on digital identity, the current situation in the USA is surprising. Perhaps motivated by a rational and considered choice, perhaps motivated by political or bureaucratic slowness. In any case, it is surprising that the world's largest economic power, as well as the seat of the largest and most important tech companies, lacks an organized discipline on digital identity. Two years ago, President Biden announced new measures aimed at preventing fraud in government benefits programs, which spiked during the pandemic in part due to identity theft. In 2023, the White House published their cybersecurity strategy, which included action items to invest in digital identity solutions and update related standards. Notably, however, the strategy's implementation plan left out digital identity.

This failure to adequately address the issue of digital identity is causing significant economic losses to the US, as well as a clear lack of protection for a fundamental right that has been increasingly threatened in recent years.

Finally, for the sake of completeness, it's worth mentioning the work of the UNCITRAL Working Group IV on Electronic Commerce, which on 7 July 2022 provided a set of model legislative provisions that legally enable the use of identity management services for online identification of physical and legal persons, thus facilitating the cross-border recognition of the use of identity management. The UNCITRAL Model Law on the Use and Cross-border Recognition of Identity Management and Trust Services (MLIT) is the first global legislative text on digital identity that sets a uniform legislative standard for promoting trust in digital trade worldwide. Indeed, considering that the Internet is a virtual space and that there are no physical borders, having international rules for the mutual recognition of national electronic identification could stimulate the use of electronic transactions.[22]

Despite significant initial efforts to address digital identity by a handful of countries it is important to highlight the ~117 countries without a government-recognized system that provides online digital identity. This means at least 3.3 billion people globally - 2.2 billion adults - live in countries with significant barriers to digital government services and the digital economy without the added convenience and access to additional opportunities available by being able to access online services and transactions that require higher levels of identity assurance. Of these 2.2 billion adults, 1.1 billion are already Internet users, suggesting a large untapped potential for the introduction of digital identity solutions to

[22] M.Zichichi, C. Bomprezzi, G. Sorrentino and M. Palmirani, 'Protecting digital identity in the Metaverse: the case of access to a cinema in Decentraland' in Proc of the 5th Distributed Ledger Technology Workshop (Bologna, Italy, 25-26 May 2023) 1.

facilitate the growth of secure online services.[23] This means that, although states are making efforts to adopt effective identification systems, many states are still behind in terms of both legislation and technology, resulting in the much-desired interoperability being far from being achieved in an environment like the metaverse, which aspires to be global.

It is important to highlight, for completeness, how the increasing use of the Regulation by design (RbD) method could help in the adoption of uniform and interoperable laws. RbD is a widespread approach to regulating digital technologies. Under this approach, the developers of digital systems must adopt technical measures that implement specific requirements mandated by law in their software. Some jurisdictions, notably the European Union (EU), have turned to regulation by design as a mechanism to automatically enforce legal requirements.[24] This method can have important implications for the law-making process. This kind of approach, among other instances, has been used for GDPR and AI Act, two of the most important EU regulations of recent years. This topic is too broad to address in this context, however, that the law cannot regulate technology without using technology itself for its purposes is worth serious consideration. The legislative response has been too slow and inefficient to keep pace with the technological development of the last few years. The consequence of which is laws already being outdated at the time of effect. Furthermore, given the international dimension of the digital world, adopting different legislative solutions could be a significant limitation. Taking inspiration from the field of fundamental rights, a possible solution could therefore be to set forth fundamental technological standards for all future developments in the field and only afterwards develop tailored solutions for each legal system.

6. Conclusion

The technological development of the last years has brought on a digital revolution with widespread societal effects comparable to the Industrial Revolution, and along with it have come numerous consequences. The widespread use of these technologies brings with it both many new opportunities as well as previously unknown dangers, and as a result, new interests worthy of protection have emerged. Among these is identity, a right that has always been understudied and undervalued. Perhaps this is because, in its simplicity, identity was a difficult concept to grasp in a world characterized exclusively in the physical dimension. Until a few years ago, it was rare to hear about "identity theft." However, in the digital dimension, this phenomenon is now a daily occurrence. Consequently, the right to personal identity, especially in the digital world, has gained much more attention. Digital identity is therefore a right that has deep roots but has only recently begun to be studied. It is still a concept in evolution, but many countries have started to pay attention to it. The strategies adopted are sometimes different, mainly due to the technical solutions chosen, however, most of the regulations adopted in various countries pursue the same goals: interoperability and security. Interoperability is essential to make the online user

[23] Calculated based on the share of Internet users in the countries without a digital identity solution for online service access, using the latest (2021/2022) data from the World Development Indicators database (https://data.worldbank.org/indicator/IT.NET.USER.ZS)

[24] M Almada, 'Regulation by Design and the Governance of Technological Futures' (2023) 14(4) European Journal of Risk Regulation 697 doi:10.1017/err.2023.37 accessed 27 May 2024.

experience simple and enjoyable and take on an even more important role in the metaverse.

Asking a user to create a separate account for each virtual world is a significant disincentive to use this technology. Furthermore, allowing a user to import tokens between different virtual worlds will be important. This is probably the biggest challenge that the metaverse will have to face alongside the development of infrastructure. As for security, the development of new technologies, probably based on blockchain, ought to help. However, the limitations encountered so far are not close to being solved, and the rights at stake are too important to people's lives to be resolved hastily. In analyzing the approaches taken by various countries highlight critical issues. First, entrusting the management of digital wallets to private entities exposes users to security risks and entrusts a huge power to digital identity service providers. On the other hand, if these services were managed by public entities or related to the state, it could create a situation of potential public authority control over citizens' identities. It is dangerous for individual rights, especially in countries where the rule of law is not guaranteed.

In conclusion, despite the initial steps taken by some countries, there are still too many without a secure identity and identification system. This leads to, among other things, discrimination against people who do not yet enjoy a system that protects their identity in a digital world where risks are numerous. The road to a unique and secure digital identity is still very long and full of challenges, but the aim is clear, a digital identity system with a high level of safety, interoperability, and ease of use.

Bibliography

Alamillo I. and Schwalm S., 'The possible impacts of the eIDAS 2.0 digital identity approach in Germany and Europe' (2023) Open Identity Summit 2023 DOI: 10.18420/OID2023_09 (Gesellschaft für Informatik e.V., Bonn) 109.

Almada M., 'Regulation by Design and the Governance of Technological Futures' (2023) 14(4) European Journal of Risk Regulation 697 doi:10.1017/err.2023.37 accessed 27 May 2024.

Doerk A., 'An introduction to self-sovereign identity (SSI)' https://ssi-ambassador.medium.com/an-introduction-to-self-sovereign-identity-ssi-916eb42f0490 accessed 27 May 2024.

Ertzscheid O., What is digital identity? (2016). OpenEdition Press. https://doi.org/10.4000/books.oep.1235.

European Union Agency for Cybersecurity, Digital Identity: Leveraging the Self-Sovereign Identity (SSI) Concept to Build Trust (2022).

Federal Trade Commission, Consumer Sentinel Network Data Book 2022 https://www.ftc.gov/reports/consumer-sentinel-network-data-book-2021 accessed 27 May 2024.

Godelli v. Italy, Application no. 33783/09 (European Court of Human Rights September 25, 2012).

Metz A. Z., Casher C. S. and Clark J. M., ID4D Global Dataset 2021: Volume 2 - Digital Identification Progress & Gaps (World Bank Group) http://documents.worldbank.org/curated/en/099020824141510923/P176341192f2c50e11bc5619be95c4fb2ed accessed 27 May 2024.

Michalkiewicz-Kadziela E. and Milczarek E., 'Legal Boundaries of Digital Identity Creation' (2022) 11(1) Internet Policy Review 113.

Mikulić v. Croatia, Application no. 53176/99 (European Court of Human Rights February 7, 2002).

Odièvre v. France, Application no. 42326/98 (European Court of Human Rights February 13, 2003).

Oyetunde B., 'The making of a giant: Estonia and its digital identity infrastructure' (2022) e-Estonia https://e-estonia.com/the-making-of-a-giant-estonia-and-its-digital-identity-infrastructure accessed 27 May 2024.

Resta G., 'Identità personale e identità digitale' (2007) Dir Informatica 511.

République française, 'FranceConnect' https://franceconnect.gouv.fr/ accessed 27 May 2024.

Sullivan C., 'Digital identity – The legal person?' (2009) 25(3) Computer Law & Security Review 227.

Sullivan C., Digital Identity: An Emergent Legal Concept (University of Adelaide Press 2011) http://www.jstor.org/stable/10.20851/j.ctt1sq5wqb accessed 27 May 2024.

Tene O., 'Me, Myself and I: Aggregated and Disaggregated Identities on Social Networking Services' (2013) 8(2) Journal of International Commercial Law and Technology 118.

Tene O., 'Me, Myself and I: Aggregated and Disaggregated Identities on Social Networking Services' (2012) Journal of International Commercial Law and Technology, SSRN https://ssrn.com/abstract=1959792 accessed 27 May 2024.

Whitley E. A., Gal U. and Kjaergaard A., 'Who do you think you are? A review of the complex interplay between information systems, identification and identity' (2014) European Journal of Information Systems 23(1) 17–35. https://doi.org/10.1057/ejis.2013.34.

World Bank, National Digital Identity and Government Data Sharing in Singapore: A Case Study of Singpass and APEX (2022) https://documents1.worldbank.org/curated/en/099300010212228518/pdf/P171592079b3e50d70a1630d5663205bf94.pdf accessed 27 May 2024.

World Economic Forum, 'Metaverse Identity: Defining the Self in a Blended Reality' (Insight Report, March 2024).

Zaccaria A., Schmidt Kessel M., Schulze R. and Gambino A. M., EU eIDAS Regulation – Article-by-Article Commentary (Beck Hart Nomos 2020).

Zichichi M., Bomprezzi C., Sorrentino G. and Palmirani M., 'Protecting digital identity in the Metaverse: the case of access to a cinema in Decentraland' in Proc of the 5th Distributed Ledger Technology Workshop (Bologna, Italy, 25-26 May 2023) 1.

MetaverseUA
Chair

Universitat d'Alacant
Universidad de Alicante