

The Legal Framework for the Protection of Digital Identity at the European Level

الإطار القانوني لحماية الهوية الرقمية على المستوى الأوروبي

*BOUKREDINE Hiba**

*Badji Mokhtar University – Annaba – Faculty of Law and Political
Science (Algeria)*

boukredinehiba@gmail.com

Orcid :

Accepted ...26../05./2025 Received 23/10/2025

• Abstract:

The protection of European digital identity is considered one of the top priorities of the European legislator, due to the importance of this right, which enables individuals to carry out various transactions on the one hand, and protects European digital sovereignty on the other—especially in light of the highly advanced technological developments taking place across Europe. In response to the threats that may affect this category of rights, Europe adopted Regulation No. 2014/1183, which establishes the European framework for digital identity. This regulation directly addresses the issue, as the European legislator seeks to strike a balance between technological progress and the protection of the components upon which digital identity is based. However, can European legal texts be considered the primary foundation for protecting digital identity? This is the question we will attempt to address in this article.

Keywords: Protection – Digital Identity – Data – Digital Environment.

المخلص:

تُعد حماية الهوية الرقمية الأوروبية من بين الأولويات القصوى للمشرع الأوروبي، نظرًا لأهمية هذا الحق الذي يمكن الأفراد من إجراء مختلف المعاملات من جهة، ويحافظ على السيادة الرقمية الأوروبية من جهة أخرى، خاصة في ظل التطورات التكنولوجية المتسارعة التي تشهدها القارة الأوروبية. واستجابةً للتهديدات التي قد تمسّ هذه الفئة من الحقوق، اعتمد الاتحاد الأوروبي اللائحة رقم 2014/1183 التي أرست الإطار الأوروبي للهوية الرقمية. وقد تناولت هذه اللائحة الموضوع بشكل مباشر، إذ يسعى المشرع الأوروبي إلى تحقيق توازن بين التقدم التكنولوجي وحماية المكونات التي تقوم عليها الهوية الرقمية. غير أنّ التساؤل المطروح هو: هل يمكن اعتبار النصوص القانونية الأوروبية الأساس الرئيس لحماية الهوية الرقمية؟ هذا ما سنحاول الإجابة عنه في هذه المقالة.

الكلمات المفتاحية: الحماية، الهوية الرقمية، البيانات، البيئة الرقمية.

• Introduction

The European human rights system is considered one of the most effective regional systems, as it relies on numerous conventions dedicated to protecting a wide range of rights that have been impacted by developments on both the international and European stages. Technological advancement has enabled individuals to enjoy a certain level of privacy in the digital space, granting them a *digital identity* that they use to represent themselves and conduct various electronic transactions available in this space. In light of this, the European Parliament has called on European states to adopt the *digital wallet*, which would allow states to both verify the identity of users and protect their personal data from potential breaches.

Significance of the Study:

The significance of this study lies in the following points:

- European conventions have kept pace with technological progress to the extent that they have recognized the individual's *digital identity*, unlike other international and regional conventions which still emphasize general privacy without such specific recognition.
- Various mechanisms operating in the field of human rights protection at the European level confirm that the right to *digital privacy* originates from the right to *digital identity*.
- The essence of preserving digital sovereignty is grounded in the state's obligation to protect the right to digital identity.

Research Objectives:

This study aims to:

- Clarify the importance of the explicit recognition of digital identity as addressed in Regulation 910/2014.
- Identify the protection mechanisms established by both the European Union and the Council of Europe to safeguard digital identity.
- Explain the relationship between digital identity protection and the implementation of the digital wallet.
- Highlight the measures taken by states to ensure the protection of digital identity within the framework of EU policy.

Research Methodologies Used:

The following methodologies were adopted:

- **Content Analysis Method:** Used to analyze various conventions concerned with the protection of digital identity, whether directly or indirectly.

- **Descriptive Method:** Employed to describe the main signs and symbols that may be used by European individuals in virtual spaces.

Research Problem:

The core research problem lies in the following question:

To what extent have international and European charters contributed to establishing a legal framework for digital identity at the European level?

I. The Legal Basis for the Protection of European Digital Identity

Ensuring the effective enjoyment of all rights—whether civil, political, economic, or cultural—for all individuals is among the primary objectives that both the Council of Europe and the European Union seek to achieve. Since the majority of international legal scholars consider the right to digital identity to occupy a special status among personal rights—given that it encompasses both the material and moral aspects of human personality—this is evidenced by numerous legal texts, both international and European, which will be addressed in this section as follows:

1. International Legal Texts as a Legal Basis for the Protection of European Digital Identity

1.1. Article 12 of the Universal Declaration of Human Rights

1.2. Article 12 of the Universal Declaration of Human Rights states: *"No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence... Everyone has the right to the protection of the law against such interference or attacks."*¹

From the above, we can conclude that the Universal Declaration of Human Rights is the foundational core of many legal norms that have been reflected in most international conventions. It is one of the declarations that affirms the basic principles upon which the protection of human rights is based, including the sanctity of private life. This right has always been associated with information technology and its various uses by individuals on one hand, and with a significant aspect of personal life on the other.²

Accordingly, contemporary international legal doctrine agrees that every individual has the right to enjoy the components of their personal data,³ the most important of which is digital identity, which has become a central pillar of financial, political, and other transactions—especially at the European level.⁴

¹ Article 12 of the Universal Declaration of 1948.

² BaraqLami, The Crime of Violating Privacy Through Electronic Means in Jordanian Legislation, A Comparative Study, Master's Thesis, University of the Middle East, Jordan, 2017, p. 59.

³ The French law No. 17-78 defines personal data in its second article as: "Information relating to a specific or identifiable natural person, either directly or indirectly, through reference to an identity number or one or more specific elements relating to them." See: Act. (2) of law 78-14 - 06/01/1978.

⁴ Contra Eynard, Les Données Personnelles, Quelle Définition Pour Un Régime Efficace?, Michalon, Paris, 2013, p. 435.

Hence, we conclude that the Universal Declaration of Human Rights is one of the most important legal pillars supporting the right to digital identity at the European level.

1.2. Article 17 of the International Covenant on Civil and Political Rights (1966)

Although Article 17 of the 1966 International Covenant on Civil and Political Rights does not explicitly mention the right to digital identity, international legal scholars affirm that electronic transactions have created a unique space for individuals. If we adopt a concept aligned with the technological developments occurring globally,¹ the right to enjoy a digital identity can be seen as falling within the scope of digital privacy. In fact, it is one of its most significant expressions. Therefore, every person has the right to exist as a *digital person* on the internet in addition to their physical existence,² and no one has the right to interfere with or violate this right, in accordance with Article 17 of the Covenant.³

To ensure additional safeguards, Article 17 of the Covenant obliges state parties to strengthen the legal framework that guarantees this right will not be violated. This is precisely what European countries have done—as we will discuss later.⁴

1.3. The Declaration on the Use of Scientific and Technological Progress in the Interests of Peace and for the Benefit of Humanity (1975)

The 1975 Declaration on the Use of Scientific and Technological Progress in the Interests of Peace and for the Benefit of Humanity is one of the key legal guarantees that can be relied upon to protect the right to digital privacy, including digital identity at the European level. This is confirmed in Article 10 of the Declaration:

*"Scientists must... respect the confidentiality of information obtained..."*⁵

And Article 9 explicitly states:

*"Every individual has the right to privacy, which includes the right to protection from arbitrary interference..."*⁶

From the above, we conclude that while the Declaration does not explicitly address digital identity, its reference to technology and scientific progress—along with today's reality of digital communication through digital identities, particularly in Europe—leads us to assert that the

¹ Salah Osman, Digital Citizenship and the Crisis of Identity, Arab Center for Research and Studies, Issue 27, 2020, pp. 19-20.

² Ghazil Aisha, "International Protection of the Right to Privacy in the Digital Domain," Al-Mi'yar Journal, Vol. 27, Issue 4, 2023, p. 411.

³ Marko Milanowc, Human Rights, Treaties, and Foreign Surveillance: Privacy in the Digital Age, Harvard International Law Journal, Vol. 56, No. 1, Winter 2015, p. 85.

⁴ Article 17 of the International Covenant on Civil and Political Rights of 1966.

⁵ Article 10, Declaration on the Use of Scientific and Technological Progress for the Benefit of Peace, 1975.

⁶ Article 9, Declaration on the Use of Scientific and Technological Progress for the Benefit of Peace, 1975.

Declaration is one of the most important legal foundations supporting the protection of digital identity in Europe.

1.4. The International Convention on the Protection of the Rights of All Migrant Workers and Members of Their Families

This is among the international conventions concerned with protecting migrant workers and their families. In its first part, it refers to the need to respect a range of rights, including the right to privacy and protection against violations¹—which, according to contemporary international legal scholarship, certainly includes digital identity, now considered a component of digital privacy. This is supported by Article 14 of the Convention, which states: *"No migrant worker or member of his or her family shall be subjected to arbitrary or unlawful interference with his or her privacy..."*

It is also worth noting that the Convention emphasizes the need for concerted international and regional efforts to ensure the protection of various rights of migrant workers and their families—including digital privacy and digital identity. Thus, the International Convention on the Protection of the Rights of All Migrant Workers and Members of Their Families² is considered one of the key legal foundations supporting the protection of digital identity at the European level, encouraging all necessary measures to prevent violations of the right to privacy, including digital identity.

From the above, we conclude that digital identity is a fundamental component of digital privacy. It is one of the most vital personal rights and must be secured, with the necessary conditions provided for its enjoyment and protection from violation.

Therefore, despite the absence of a clear and explicit international text, most legal scholars affirm that digital identity is indeed protected by human rights instruments, particularly those that guarantee the right to privacy.³

2. International Resolutions Supporting the Protection of Digital Identity in Europe

Given the significance of digital privacy and its relevance to various interactions, many international resolutions and recommendations have emphasized the need to protect it. Notable examples include:

2.1. United Nations General Assembly Resolution on the Right to Privacy in the Digital Age (18/12/2013):

¹ Nora Issa Zakaria Abdelsalam, "Constitutional Protection Mechanisms for the Sanctity of Private Life in the Age of Technology," *Journal of Legal and Economic Studies*, Faculty of Law, Vol. 09, September 2022-2023, pp. 751-752.

² Amna Ben Taher, "International Protection of Migrant Workers' Rights within the Framework of the International Labour Organization and the International Convention for the Protection of Migrant Workers and Their Families," *Journal of Humanities*, Vol. 7, Issue 2, June 2022, pp. 109-110.

³ Emmanuel Netter, *Digital and Fundamental Concepts of Private Law*, CEPRIXA, France, 2019, pp. 135-138.

This resolution stresses the importance of not violating the right to digital privacy, including personal data,¹ which reflects a person's digital identity—a collection of attributes, symbols, and identifiers used to represent oneself in virtual space and communicate with others.

To strengthen the protection of digital identity in Europe, based on this Resolution No. 68/167 and others that will be mentioned later, the European Union adopted a regulation specifically addressing this right.

2.2. Human Rights Council Resolution No. 32/20 (27 June 2016):

During its 32nd session, titled "*The Promotion, Protection, and Enjoyment of Human Rights on the Internet*", this resolution affirms the need to respect all rights that individuals enjoy offline—including personal data protection and, certainly, digital identity—particularly emphasized in paragraph 08.²

2.3. General Assembly Resolution No. 71/199 on the Right to Privacy in the Digital Age (25 January 2017):

This resolution stresses the need to protect privacy in the digital space—now referred to as digital privacy—which includes digital identity. It specifically states: "*Metadata, when collected, can reveal personal information and provide a profile of... a person's identity.*"³

This has prompted European countries to move toward adopting what is now called a *digital wallet*.

2.4. Human Rights Council Resolution No. A/HRC/29/39 (3 August 2013):

This resolution explicitly affirms the need to ensure protection of digital identity, which falls under the umbrella of privacy, as noted in paragraph 6.⁴

2.5. Human Rights Council Resolution No. 31/48 (13 September 2021):

This resolution focuses on the right to privacy in the digital age,⁵ highlighting the increasing impact of artificial intelligence on the enjoyment of privacy and associated rights, including digital identity. It calls for safeguards to stop the sale and use of AI in ways that could significantly harm human rights in general.

¹ General Assembly Resolution No. 67/168, The Right to Privacy in the Digital Age, dated December 18, 2013, Session 68, pp. 1-3.

² Session 32, Human Rights Council, No. L20/32/A/HRC, dated June 27, 2016, pp. 4-5.

³ Session 71, General Assembly, No. 199/71/A/RFS, dated January 25, 2017, p. 4.

⁴ Session 39, Human Rights Council, No. 29/39, dated August 3, 2018, pp. 4-6.

⁵ Session 50, Human Rights Council, Annual Report of the United Nations High Commissioner for Human Rights No. 31/48 A/HRC, dated September 13, 2021, pp. 4-6.

2.6. General Assembly Resolution No. 29/173:

This resolution includes the report of the Special Rapporteur on the right to privacy, which proposed updating General Assembly Resolution 45/95 titled “*Guidelines for the Regulation of Computerized Personal Data Files.*”

This report is significant because it explicitly addresses internet identity or digital identity, which identifies individuals in digital interactions, by promoting the adoption of several key principles by states, including:

- Principle of lawfulness and fairness
- Principle of data accuracy and quality
- Principle of purpose limitation, necessity, proportionality, and temporariness
- Principle of effective protection of data subjects’ rights
- Principle of confidentiality¹

These principles have pushed many countries—especially in Europe—to formally recognize digital identity and to provide robust frameworks for its protection.

3. European Conventions and Resolutions as a Legal Basis for the Protection of European Digital Identity

In addition to international agreements directly related to the protection of human rights, including the protection of personal data in the digital space—of which digital identity is undoubtedly a fundamental component—European agreements and decisions have gradually and explicitly recognized digital identity as an independent right within a European framework. Accordingly, we will address the progressive and explicit recognition of this important right by European countries as part of digital rights.

3.1. The European Convention on Human Rights of 1950:

Digital identity is protected within the framework of texts concerned with human rights protection at the European level, including the European Convention on Human Rights of 1950. Therefore, the protection of digital identity is guaranteed from the perspective of the right to privacy, as private life has extended to the digital space, where individuals interact with others through their digital identity.²

3.2. The Treaty on the Functioning of the European Union (TFEU):

¹ For more information, see: "Special Rapporteur's Report on the Right to Privacy No. 173/79, dated July 17, 2014, Session 79 of the General Assembly."

² Valentin Rupy, Max Crafenstein, Clarifying "Personal Data and the Role of Anonymisation in Data Protection Law: Including and Excluding Data from the Scope of the GDPR (More Clearly) Through Refining the Concept of Data Protection," *Computer Law and Security Review*, Vol. 52, 2024, p. 8.

The Treaty on the Functioning of the European Union, signed on December 13, 2007, and entering into force in 2009, is one of the most important treaties that explicitly referred in Article 16 to the need to protect personal data related to individuals.¹ Since digital identity is essentially a projection, in one way or another, of personal identity used for interaction, European countries are obligated to provide protection for it through legislative texts.

3.3. Convention 108 of the Council of Europe:

The Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, which has undergone multiple amendments to keep pace with technological advancements (the latest of which entered into force on May 25, 2018), is one of the most important regional instruments in the field of data protection because:

3.1.1. It aims to achieve two main objectives:

- To address the challenges arising from the use of new information and communication technologies.
- To strengthen the effective implementation of the Convention.²

3.1.2. It protects the data of all EU citizens regardless of their nationality or place of residence.

3.1.3. Among the types of data covered by Convention 108 are genetic data, personal data related to crimes, convictions and security measures, and biometric data identifying individuals.

Therefore, European states are obligated to protect digital identity through the protection of personal data, as evidenced by Article 4 of Convention 108 and the jurisprudence of the European Court of Justice, which confirmed the strong link between personal data and identity, including digital identity,³ in pursuit of the recognition of the "right to informational self-determination."

3.4. The Charter of Fundamental Rights of the European Union of 2000:

Digital identity enjoys protection under the Charter of Fundamental Rights of the European Union from the perspective of personal data protection, as evidenced by Article 07 of the Charter.

3.5. The Budapest Convention on Cybercrime:

¹ See: Article 16, Official Journal of the European Union, Consolidated Version of the Treaty on the Functioning of the European Union, C326/47, 26/10/2012, p. 9.

² Paul M. Schwartz and Karl NikolausPeifre, Structuring International Data Privacy Law, Georgetown Law Journal, Vol. 12, Issue 2, May 2022, p. 18.

³ Michele Finck and Frank Pallas, "They Who Must Not Be Identified: Distinguishing Personal from Non-Personal Data Under the GDPR," International Data Privacy Law, Vol. 10, No. 1, pp. 11-36.

The Budapest Convention on Cybercrime of 2004 is one of the most important European regional agreements that emphasizes the necessity of protecting digital rights, including those affecting or related to individual privacy, such as digital identity. This is demonstrated by the preamble of the Convention, which states: “...emphasizes the protection of rights related to the automated processing of personal data”,¹ and Article 02 of the 2004 Budapest Convention, which considers unauthorized access to a computer to obtain personal information or access data stored on the device a violation of digital privacy.²

It is also worth noting that the Convention does not only stress the need to take national and regional legislative measures to protect digital privacy, including digital identity, but also goes further by emphasizing the necessity of cooperation in the event of legal proceedings³ against individuals committing violations of digital privacy, including the digital identity of European citizens.⁴

3.6. Regulation No. 1183/2024 on the European Framework for Digital Identity:

Regulation (EU) 2024/1183 of the European Parliament and of the Council of 11 April 2024 amending Regulation (EU) No 910/2014 as regards the establishment of the European framework for a digital identity

Regulation No. 1183/2024 is one of the most explicit and foundational legal texts dedicated to the protection of digital identity at the European level. Therefore, we will address several key points related to this regulation, including the supporting regulations, its purpose, and the main issues it addresses.

4. Regulations Underpinning Regulation 1183/2024

4.1. Regulation No. 2014/910 concerning electronic identification and trust services for electronic transactions in the internal market, issued by both the European Parliament and the Council of the European Union. This regulation aimed to establish a new system for electronic interaction and to eliminate barriers through the use of electronic identity, thereby promoting trust in electronic transactions and enhancing the quality of commercial dealings.

This regulation was the foundation upon which Regulation 1183/2024 was built, having been amended on April 11, 2024.⁵

4.2. Regulation No. 679/2016 issued by the European Parliament and Council on April 27, 2016, concerning the protection of natural persons with regard to the processing of personal data

¹Alali Abdallah Ahmed, Transnational Cybercrime - Methods of Combatting According to the Budapest Convention, Al-Nahda Publishing, Egypt, 2007, p. 22.

² See also, Azzam Al-Hayt Adel, Defamation and Insult Crimes Committed via Electronic Media, Dar Al-Thaqafa, Jordan, 2019, pp. 381-383.

³ Council of Europe, Preamble, Cybercrime Convention 2001, Entered into Force 2004.

⁴ See Article 2, Cybercrime Convention, for more information, see Qattaf Suleiman, Bougrine Abdelhalim, Legal Mechanisms for Combatting Cybercrimes under the Budapest Convention, Academic Journal of Legal and Political Research, Laghouat, Vol. 6, Issue 1, 2022, pp. 341-342.

⁵ Vincent Michelles, Understanding, Journal of Communication, Vol. 16, 2022, pp. 3846-3847.

and the free movement of such data. This regulation is considered one of the most important legal texts regarding the protection of personal data for EU citizens, enshrining several key legal principles that impact individuals, European states, and the legal and doctrinal fields.¹

Its importance lies in addressing:

The right to informational autonomy, whereby individuals have the right to control their personal data and can decide whether to disclose, exploit, or use it.² This is outlined in Article 7.

However, it also maintains the state's role in protecting its digital sovereignty against individuals, which led European countries to adopt a unified European framework to protect digital identity.

- The right to be forgotten, allowing individuals to delete their data upon request.
- The right to data portability between service providers.³

In this regard, we refer to other regulations upon which Regulation (1183/2024) is based:

- 4.3. Regulation (1725/2018) issued by the European Parliament and Council concerning:
- 4.4. *Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices, and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC*, which pertains to the protection of individuals in relation to the processing of personal data by the Union's institutions, bodies, and agencies, and to the freedom of movement.
- 4.5. Regulation (881/2019) concerning cybersecurity certification for information and communication technology.
- 4.6. *Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification, and repealing Regulation (EU) No 526/2013 (Cybersecurity Act)*
- 4.7. Regulation (1157/2019) regarding the enhancement of identity card security for EU citizens and residence documents issued to EU citizens and their family members exercising their right to free movement.

¹ Official Journal of the European Union, 1257, Regulation (EU) No. 909/2014 of the European Parliament and the Council of July 23, 2014, Concerning the Improvement of Securities Regulation in the European Union and Central Securities Depositories, and Amending Directives 98/26/EC and 2014/65/EU as well as Regulation (EU) No. 236/2012, Text Presenting Interest for the EEA.

²Namly. Al-Ashqar, Jamal Mazzour, International and European Legislation for the Protection of Personal Data, Journal of Damascus University for Legal Sciences, Vol. 1, Issue 2, 2021, pp. 231-232.

³ Pauline Turk, Informational Self-Determination: An Emerging Fundamental Right?, Dalloz, France, 2020, pp. 616-620.

- 4.8. *Regulation (EU) 2019/1157 of the European Parliament and of the Council of 20 June 2019 on strengthening the security of identity cards of Union citizens and of residence documents issued to Union citizens and their family members exercising their right to free movement*
- 4.9. Commission Recommendation (EU) (946/2021) issued on 3 July 2021 on the EU common toolbox for a coordinated approach and a framework for the European digital identity.
- 4.10. *Recommendation (EU) 2021/946 of the Commission of 3 June 2021 on a common Union toolbox for a coordinated approach towards a European framework for a digital identity*
- 4.11. Regulation (1925/2022) issued on 14/09/2022 on contestable and fair markets in the digital sector.¹
- 4.12. *Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act)*

5. Objectives of Regulation (1183/2024):

Following the adoption of Regulation (1183/2024) on 11/04/2024 and its entry into force on 20 May 2024, the European Parliament and the Council aim to achieve the following objectives:

- 5.1. Providing the European Digital Identity Wallet *Portefeuille européens d'identité numérique*.
- 5.2. Enhancing protective guarantees for the digital identity or what is known as internet identity.
- 5.3. Providing digital services across the European continent in both the public and private sectors.

6. Key points included in the Regulation:

Regulation (1183/2024) includes several critical points as follows:

- 6.1. The European Digital Identity Wallet *Portefeuille européens d'identité numérique*, which consists of a set of data for any European person—natural or legal—while maintaining the right to individual sovereignty over their data.
- 6.2. Mutual recognition of national electronic identification systems.
- 6.3. Trusted services, where digital services are offered transparently to all natural and legal persons.²

II. Foundations of the European Digital Identity under Legal Protection

According to international jurisprudence, personal data has taken on a dual dimension and has become one of the most important components of identity in its digital aspect, as it serves as a

¹ Marie Martin, "Emerging Rights in the Era of the Right to Informational Self-Determination," *Politien*; November 2017; No. 31, pp. 251-261.

² eur-lex.europa.eu/legal-content/FR/TXT/celex/32024/R/1183.

means of identifying a person conducting transactions electronically across various domains in cyberspace.¹ However, Regulation (1183/2024) also explicitly confirms this legal trend in Article 3, Paragraph 54, by referring us to Article 4, Paragraph (1) of Regulation (679/2016).² Accordingly, we will address the personal data under protection, which constitutes the main foundation of digital identity, as well as the data excluded from this protection as they do not constitute essential elements of digital identity.

1. Personal data as a foundational element of the European digital identity

Upon reviewing Article 4 of Regulation (679/2016), we conclude that personal data includes all information related to any person through which the person can be identified directly or indirectly, such as: name, personal image, biometric or genetic data, email address, license numbers, personal property, bank account numbers, fetal records, memory card... etc.

In this regard, we refer to a doctrinal definition of personal data as data that is processed to achieve a specific goal or for specific use in decision-making. It is data that gains value after being analyzed, interpreted, or compiled into meaningful form and can be circulated, recorded, published, and distributed formally or informally in any format.

Thus, personal data is one of the primary foundations of digital identity because it is:

- Data or a set of rights related to the private life of a natural or legal person.
- Allows the identification of the individual being dealt with (most legislations consider elements of civil, physiological, genetic, psychological, economic, cultural, and social identity among the main components of personal data).³

From the above, we conclude that maintaining the European digital identity is linked to the right to privacy, in the same way that privacy is based on special protection. Preserving identity, which may involve numerous variables essential to life and constitutive of the right's subject, thus begins.

Hence, the relationship between privacy and identity is a special legal relationship between the individual and the objective and subjective criteria that express personal identity.⁴

Given the importance of data as a vital component of digital identity—as per Article 4 (Para. 2) of Convention 108⁵ and Article 4 (Para. 2) of Regulation (1183/2024) on the European digital identity

¹ See: Regulation (EU) 2024/1183 of the European Parliament and the Council of April 11, 2024, Amending Regulation (EU) No. 910/2014 Concerning the Establishment of the European Framework for Digital Identity.

² Julien Pierre, "Genetics of Digital Identity: The Calves of Digital," Vol. 7, 2011/1, pp. 15-19.

³ See: Article 4 (54), Regulation (EU) 2024/1183 of the European Parliament and the Council of April 11, 2024, Amending Regulation (EU) No. 910/2014 Concerning the Establishment of the European Framework for Digital Identity.

⁴ Michel Finck and Frank Pallas, Act. Pre, pp. 12-13.

⁵ Jean Christophe Saint Pau, Personality Law, Lexis Nexis, Paris, 2013, pp. 559-561.

framework (4)¹—European countries are required to process personal data electronically. Every operation or set of operations performed with or without automated means and applied to personal data such as collection, registration, organization, structuring, storage, alteration, extraction, consultation, use, communication by transmission or dissemination, or any other form of availability, alignment, linking, erasure, or destruction...²

Processing may be automated, whether partially or wholly, using modern technologies such as computers, software, mobile devices, artificial intelligence technologies, etc.³

Some data may also be subject to non-automated processing using traditional tools such as records, notebooks, memos, and archiving data in structured paper files.⁴

Despite the variation between automated and non-automated processing, personal data may be exposed to threats or violations, whether by the state or certain individuals. These violations depend on the sensitivity of the personal information and the technologies used in the processing. Violations may target the purpose of processing personal data.

Therefore, European countries are required to protect personal data⁵ in accordance with the principles outlined in Convention 108, which include: lawfulness, fairness, transparency, purpose limitation (before employment), data minimization, data accuracy, storage limitation, integrity and confidentiality, and accountability.⁶

2. Sensitive Data

In addition to ordinary and personal data, there exists inherently sensitive data that may pose risks to its holders and requires enhanced protection. According to Article 09 of Regulation (679/2016) and Article 09 of Regulation (1183/2024), this data includes:

- Personal data revealing racial or ethnic origin
- Personal data revealing political, religious, or other beliefs, including philosophical ones
- Personal data revealing trade union membership
- Genetic and biometric data processed to identify a person
- Personal data related to health, sexual life, or sexual orientation⁷

Article 10 of Regulation (679/2016) also refers to another category of sensitive data, namely personal data related to crimes and criminal convictions. However, when referring to both Articles

¹ See: Art (4,2) of Regulation (EU) 2016/679.

² See: Art (4,2) of Regulation (EU) 2024/1183.

³ See: Art (4,2) of Regulation (EU) 2016/679.

⁴ Michelle Bachelet Jeria, Human Rights and the Digital Balance: Can They Change Things? Keynote Address by Michelle Bachelet, UN High Commissioner for Human Rights, Japan Society, New York, October 17, 2019, available at the following link: <https://www.ohchr.org/fr/2019/10/keynote-address-un-high-commissioner-human-rights-michelle-bachelet>.

⁵ Mona Al-AshqarHiyour, "Surveillance, the Obsession of the Era," Arab Center for Legal and Judicial Research, Beirut, 2016, pp. 100-102.

⁶ WasimShafiq Al-Hijar, Legal System for Social Media, Arab Center for Legal and Judicial Research, Beirut, 2018, p. 67.

⁷ See: Art (5 bis), Regulation (EU) 2024/1183.

9 and 10 of European Regulation (679/2016),¹ not all listed types of data are subject to processing, since such processing may pose a direct threat to individual rights and freedoms due to the sensitive nature of the data.²

Therefore, according to international doctrine, this type of data is excluded from the right to informational self-determination, as its processing is subject to specific procedures with special instructions.³ On the other hand, the processing of personal data is carried out in accordance with the provisions of Regulation (679/2016), Regulation (1183/2024), and Regulation (628/2025) issued on 31 March 2025, concerning internal rules for informing data subjects and restricting certain data subject rights in the context of processing by the Commission for purposes of supervision, investigation, enforcement, and control under Regulation (EU 2065/2022).⁴

From the above, we conclude that data is one of the most important pillars of a European person's digital identity. However, the European individual enjoys several privileges, including:

- 2.1. Right to access data:** Based on the right to informational self-determination, individuals have the right to access their data and monitor the data being processed. This is evidenced in Article 15 of Regulation (679/2016) and Article 05 of Decision (628/2025).⁵
- 2.2. Right to rectification:** According to Article 16 of Regulation (679/2016) and Decision (628/2025), the individual controlling the data has the right to correct inaccurate or incomplete data.⁶
- 2.3. Right to be forgotten:** The digital right to be forgotten is enshrined as an essential element of informational self-determination, allowing individuals to delete their personal data from social media platforms and search engines. This is confirmed by Article 19 of Regulation (679/2016) and Article 05 of Decision (628/2025).⁷

In addition to the aforementioned rights, other doctrinally agreed-upon rights exist, including: restriction of processing, data portability, and the right to object.

Thus, although individuals possess the authority to exercise informational self-determination over data—which is the core of digital identity—Regulation (1183/2024) has removed the provisions

¹ See: Art (5), Regulation (EU) 2024/1183, and Art (5), Regulation (EU) 2024/1183.

² See: Art 9, Regulation (EU) 2016/679.

³ Saleem Abdullah Souri, Legal Protection of Internet Network Information, Halabi Legal Publications, Beirut, 2011.

⁴ For more information, see: Ahmed Mohamed Mohamed Abdel-Ghaffar, The Principle of Digital Sovereignty over Data, Journal of Jurisprudential Research, Faculty of Sharia and Law in Damanhour, Issue 43, 2023, pp. 725-728.

⁵ See: Decision (EU) 2025/628 of the Commission, March 31, 2025, Establishing Internal Rules for Communicating Information to Concerned Persons and Limiting Certain Rights of Concerned Persons Regarding the Processing of Personal Data by the Commission for Surveillance, Investigation, Enforcement, and Monitoring under Regulation (EU) 2022/2065.

⁶ See: Art 15, Regulation (EU) 2016/679, and see: Art 5, Decision (EU) 2025/628.

⁷ See: Art 16, Regulation (EU) 2016/679, and see: Art 5, Decision (EU) 2025/628.

relating to these privileges. However, it introduced a series of mechanisms that offer enhanced protection of the European digital identity, including:

- Monitoring the functioning of the European digital identity wallets under Article 46 (1).
 - Control over services that must be trust-based, especially when dealing with other European countries under Article 46 (2).
 - Facilitation and cooperation in communication through governmental or non-governmental bodies among European countries, as per Article 46 (Para. 4).
 - Supervision of digital identity protection through the "European Digital Identity Cooperation Group" *Groupe de coopération européenne en matière d'identité numérique*, which acts as an observer at the ENISA Agency under the name *groupe de opération*.¹
- **Conclusion:**

Both the European Union and the European Commission have adopted a special regulation governing the European digital identity due to its importance in interactions among European citizens. It serves as an electronic means of identification. However, discussing this topic has led to several important findings and a set of suggestions.

Findings

Through the research presented, several key findings have emerged, the most important of which are:

1. The protection of the European digital identity is grounded in international legal texts related to privacy and in various instruments concerning the protection of personal data, whether they are international or European agreements or decisions.
2. The digital identity is essentially a projection, in one way or another, of the personal identity. Therefore, data is considered one of the most crucial pillars of the digital identity.
3. The right to informational self-determination has established a new concept in the relationship between an individual and their data, as it grants each person a degree of autonomy in managing their personal data by reinforcing individuals' consent and affirming the new digital rights of concerned individuals in the electronic space.
4. The use of the digital wallet is voluntary rather than mandatory for European citizens, which may hinder its alignment with technological developments, especially in digitally advanced countries such as Estonia.

Second : Recommendations

1. It is necessary to amend Regulation 2024/1183 by including the main essential elements that must be present within the digital wallet, as the current ambiguity and reference to Regulation 679/2016 result in contradictions, especially since the latter has omitted provisions related to certain rights arising from the right to informational self-determination.

¹See: Art 46, Regulation (EU) 1183/2024.

2. Provisions must be added to protect European individuals who do not possess a digital identity wallet.
3. Monitoring mechanisms should be adopted to oversee investigations in case of violations of the European digital wallet.

Bibliography:

Books:

- Alali Abdallah Ahmed, Transnational Cybercrime - Methods of Combatting According to the Budapest Convention, Al-Nahda Publishing, Egypt, 2007.
- Azzam Al-Hayt Adel, Defamation and Insult Crimes Committed via Electronic Media, Dar Al-Thaqafa, Jordan, 2019.
- BaraqLami, The Crime of Violating Privacy Through Electronic Means in Jordanian Legislation, A Comparative Study, Master's Thesis, University of the Middle East, Jordan, 2017.
- Contra Eynard, Les Données Personnelles, Quelle Définition Pour Un Régime Efficace?, Michalon, Paris, 2013.
- Emmanuel Netter, Digital and Fundamental Concepts of Private Law, CEPRIXA, France, 2019.
- Jean Christophe Saint Pau, Personality Law, Lexis Nexis, Paris, 2013.
- Mona Al-AshqarHiyour, "Surveillance, the Obsession of the Era," Arab Center for Legal and Judicial Research, Beirut, 2016,.
- Salah Osman, Digital Citizenship and the Crisis of Identity, Arab Center for Research and Studies, Issue 27, 2020.
- Saleem Abdullah Souri, Legal Protection of Internet Network Information, Halabi Legal Publications, Beirut, 2011.
- Wasim Shafiq Al-Hijar, Legal System for Social Media, Arab Center for Legal and Judicial Research, Beirut, 2018.

Articles:

- Ahmed Mohamed Mohamed Abdel-Ghaffar, The Principle of Digital Sovereignty over Data, Journal of Jurisprudential Research, Faculty of Sharia and Law in Damanhour, Issue 43, 2023.
- Amna Ben Taher, "International Protection of Migrant Workers' Rights within the Framework of the International Labour Organization and the International Convention for the Protection of Migrant -Workers and Their Families," Journal of Humanities, Vol. 7, Issue 2, June 2022.
- Ghazil Aisha, "International Protection of the Right to Privacy in the Digital Domain," Al-Mi'yar Journal, Vol. 27, Issue 4, 2023.
- Julien Pierre, Genetics of Digital Identity: The Calves of Digital, Vol. 7, 2011/1.

- Marie Martin, Emerging Rights in the Era of the Right to Informational Self-Determination, Politien; November 2017; No. 31.
- Marko Milanowc, Human Rights, Treaties, and Foreign Surveillance: Privacy in the Digital Age, Harvard International Law Journal, Vol. 56, No. 1, Winter 2015.
- Michele Finck and Frank Pallas, "They Who Must Not Be Identified: Distinguishing Personal from Non-Personal Data Under the GDPR," International Data Privacy Law, Vol. 10, No. 1.
- Nora IssaZakariaAbdelsalam, "Constitutional Protection Mechanisms for the Sanctity of Private Life in the Age of Technology," Journal of Legal and Economic Studies, Faculty of Law, Vol. 09, September 2022-2023.
- Paul M. Schwartz and Karl NikolausPeifre, Structuring International Data Privacy Law, Georgetown Law Journal, Vol. 12, Issue 2, May 2022.
- Qattaf Suleiman, BougrineAbdelhalim, Legal Mechanisms for Combatting Cybercrimes under the Budapest Convention, Academic Journal of Legal and Political Research, Laghouat, Vol. 6, Issue 1, 2022.
- Valentin Rupy, Max Crafenstein, Clarifying "Personal Data and the Role of Anonymisation in Data Protection Law: Including and Excluding Data from the Scope of the GDPR (More Clearly) Through Refining the Concept of Data Protection," Computer Law and Security Review, Vol. 52, 2024.

Legal and Official Texts:

- The French law No. 17-78 defines personal data in its second article as: "Information relating to a specific or identifiable natural person, either directly or indirectly, through reference to an identity number or one or more specific elements relating to them.

international agreement:

- Universal Declaration of 1948.
- the International Covenant on Civil and Political Rights of 1966.
- Declaration on the Use of Scientific and Technological Progress for the Benefit of Peace, 1975.
- Council of Europe, Preamble, Cybercrime Convention 2001, Entered into Force 2004.

Decisions and reports:

- Official Journal of the European Union, Consolidated Version of the Treaty on the Functioning of the European Union, C326/47, 26/10/2012.
- General Assembly Resolution No. 67/168, The Right to Privacy in the Digital Age, dated December 18, 2013, Session 68.
- Regulation (EU) No. 910/2014 Concerning the Establishment of the European Framework for Digital Identity.

- Special Rapporteur's Report on the Right to Privacy No. 173/79, dated July 17, 2014, Session 79 of the General Assembly.
- Regulation (EU) 2016/679.
- Session 32, Human Rights Council, No. L20/32/A/HRC, dated June 27, 2016.
- Session 71, General Assembly, No. 199/71/A/RFS, dated January 25, 2017.
- Session 39, Human Rights Council, No. 29/39, dated August 3, 2018.
- Michelle Bachelet Jeria, Human Rights and the Digital Balance: Can They Change Things? Keynote -Michelle Bachelet, UN High Commissioner for Human Rights, Japan Society, New York, October 17, 2019, available at the following link:
<https://www.ohchr.org/fr/2019/10/keynote-address-un-high-commissioner-human-rights-michelle-bachelet>.
- Session 50, Human Rights Council, Annual Report of the United Nations High Commissioner for Human Rights No. 31/48 A/HRC, dated September 13, 2021.
- Regulation (EU) 2024/1183 of the European Parliament and the Council of April 11, 2024, Amending Regulation (EU) No. 910/2014 Concerning the Establishment of the European Framework for Digital Identity-
- Decision (EU) 2025/628 of the Commission, March 31, 2025, Establishing Internal Rules for - Communicating Information to Concerned Persons and Limiting Certain Rights of Concerned Persons Regarding the Processing of Personal Data by the Commission for Surveillance, Investigation, Enforcement, and Monitoring under Regulation (EU) 2022/2065.

Website:

- eur-lex.europa.eu/legal-content/FR/TXT celex: 32024/R 1183.