

Fragmented Identities: Legal Challenges of Digital Identity, Integrity, and Informational Self-Determination

Lusine Vardanyan, Ondrej Hamulák & Hovsep Kocharyan*

Summary: Informational self-determination is a crucial legal principle that grants individuals greater control over their digital existence. This paper examines the complexities of digital identity and the legal challenges it presents. Digital identity blends objective elements, such as official documentation, with subjective aspects like personal and cultural affiliations. The increasing overlap between physical and digital identities raises legal and ethical concerns regarding identity protection, consent, and anonymity. The fragmentation of digital identity, risks of identity theft, and the expansion of digital profiling highlight the need for stronger legal mechanisms. While existing laws like the GDPR offer some protection, a broader legal framework is required to recognise identity as a fundamental right. The right to be forgotten and control over one's digital self-representation are essential for personal autonomy. The study underscores how digital identity is increasingly shaped by third parties, leading to vulnerabilities that threaten fundamental rights. Expanding current privacy laws through the doctrine of informational self-determination is crucial for safeguarding identity in the evolving technological landscape.

Keywords: digital identity, bodily integrity, anonymity, identity theft, informational self-determination, data protection, profiling, legal frameworks, personal autonomy, cyber law

Citation: VARDANYAN, L., HAMULÁK, O., KOCHARYAN, H. Fragmented Identities: Legal Challenges of Digital Identity, Integrity, and Informational Self-Determination. *European Studies – the Review of European law, Economics and Politics*. 2024, vol. 11, no. 1, pp. 105–121, DOI: 10.2478/eustu-2024-0005.

* *Lusine Vardanyan* is a PhD Candidate at the Department of International and European Law at the Faculty of Law at Palacký University Olomouc, Czech Republic. *Ondrej Hamulák* (corresponding author) is a senior lecturer at the Faculty of Law, Palacký University Olomouc (Czech Republic) and an adjunct professor in digital constitutionalism at School of Business and Governance, Tallinn University of Technology (Estonia). He is a member of ENDE – European Network on Digitalization and E-governance, Jean Monnet Networks no. 101127038. Contact: ondrej.hamulak@upol.cz; ondrej.hamulak@taltech.ee *Hovsep Kocharyan* is a post-doctoral researcher at the Faculty of Law, Palacký University Olomouc, Czech Republic.

Acknowledgment: This work is funded by the project no. IGA_PF_2023_014 “Data protection and personal integrity on the Internet of Bodies: New challenges for the EU law” (PI: Lusine Vardanyan) and project no. IGA_PF_2024_010 “Forming of Catalogues of Digital Human Rights” (PI: Ondrej Hamuřák), both funded by the Palacký University Olomouc IGA projects scheme.

1. Introduction

The right to informational self-determination plays a decisive role in defining and protecting personal identity in the digital space. As Luciano Floridi argues in *The Fourth Revolution*, digital identity represents a profound expansion of human ontology, integrating both objective and subjective aspects of personality.¹

While objective identity is legally recognised through official documents, subjective identity reflects an individual’s personal, political, cultural, and philosophical affiliations. The digital transformation has fundamentally blurred the boundaries between real and digital identity, rendering the latter an integral and increasingly complex dimension of individual existence.

With the exponential growth of digital technologies, concerns regarding digital identity protection have intensified.² Drawing on Helen Nissenbaum’s concept of “contextual integrity”³, the ability of third parties to construct, manipulate, and weaponise digital identities without explicit consent raises serious legal and ethical challenges. Shoshana Zuboff’s groundbreaking work on surveillance capitalism provides critical insight into how personal data is systematically extracted and monetised, further complicating the landscape of digital identity.⁴

The fragmentation of digital identity, growing risks of identity theft, and the pervasive expansion of digital profiling emphasise an urgent need for a strong legal framework to safeguard digital identity and ensure informational self-determination. This paper examines these critical concerns and explores existing and potential legal mechanisms aimed at preserving identity in the increasingly complex digital age.

¹ FLORIDI, L. *The Fourth Revolution: How the Infosphere is Reshaping Human Reality*. Oxford: Oxford University Press, 2014.

² See generally ELLIOTT, A. (ed.). *The Routledge Social Science Handbook of AI*. London: Routledge, 2021.

³ NISSENBAUM, H. *Privacy in Context: Technology, Policy, and the Integrity of Social Life*. Stanford: Stanford University Press, 2010.

⁴ ZUBOFF, S. *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*. London: Profile Books, 2019.

2. The right to informational self-determination as a mechanism for the provision of personal identity

The right indicated in the title of this section can be considered from two situations: on the one hand, it can be considered as a mechanism for creating digital identity, and, on the other hand, as a mechanism for protecting personal identity. We note that personal identity consists of two main components: 1) the right to be identified with a person's identity reflected in official documents (objective identity), and 2) the right to protect the person with whom a person wants to be associated, as arising from his/her political, cultural, philosophical and religious beliefs, as well as from his/her behaviour (subjective identity)⁵. At the same time, subjective and objective identity are closely related, since a person's subjective (personal) beliefs may well make it possible to identify his/her 'official' objective identity.

However, the concept of identity in the digital world is very difficult to define. It adds even more complexity to legal issues in the field of human protection, due to the multiplicity of different characteristics and forms inherent in it. It can be singular/multiple, identical/different, fixed/flexible, fragmented/connected, public/private, temporary/permanent, etc. Despite the fact that some researchers highlight that there is a structural difference between real and digital identity, pointing out that real identity is characterised by physical characteristics, while digital identity does not possess them,⁶ we believe that this difference between "real" and digital identities is disappearing and a person already perceives digital identity as the most important, and sometimes an inseparable part of his/her self. As pointed by Rowena E. Rodrigues⁷, this is confirmed by the European Parliament's recommendation on strengthening security and fundamental freedoms on the Internet, which recognises that digital identity is increasingly becoming an integral part of the individual.⁸ In any case, there is a real person behind the digital identity – the individual with whom it is associated or whom it represents. Therefore, digital identity should be considered as a digital interpretation of a real person.

At the same time, expanding the possibility of constructing digital subjective identity through the provision of real personal data may be contradictory to one's civil identity, which aims to identify with the help of human data. Indeed, digital

⁵ ZACCARONI, G. Fundamental rights and disruptive technologies: a right to personal identity under the European multi-level system of protection? *Freedom, Security & Justice: European Legal Studies*. 2020, no. 3, pp. (155) 143–166. DOI: 10.26321/G.ZACCARONI.03.2020.06.

⁶ ROBLES-CARRILLO, M. Digital identity: an approach to its nature, concept, and functionalities, *International Journal of Law and Information Technology*. 2024, vol. 32, no. 1.

⁷ RODRIGUES, R. E. Revisiting the legal regulation of digital identity in the light of global implementation and local difference. The University of Edinburgh, Dissertation collection, 2011, p. 55 [online]. Available at: <https://era.ed.ac.uk/handle/1842/8942>

⁸ European Parliament recommendation of 26 March 2009 to the Council on strengthening security and fundamental freedoms on the Internet (2008/2160(INI)).

identity undermines objective identity, since objective data that allows stable digital identification does not always exist. For example, by connecting to a VPN, the IP address, i. e. the “threshold” of the user’s digital existence, changes. At the same time, the IP address will no longer be stable data: identification is no longer possible using a civil identity, given that digital identification only allows for the “individualisation” of a person. Here we see all the consequences of the collapse of the principle of the immutability of the status of the individual.

The creation of digital identity of a person is not only in fact the prerogative of the person himself/herself. The advent of the IoT and IoB are changing and expanding the ways and tools of expressing, representing and projecting a person’s identity from third parties, especially for marketing, which is typical for business on the Internet. Some scholars argue that the existing law is not construed to accompany the steady progression toward the IoB, while the IoT is challenging the traditional construct of ownership, and users are progressively losing control over their IoT devices, which in turn raises the problem of balancing of technological progress and vital human safety and integrity of human bodies in digital world.⁹ Moreover, the creation of a digital profile of a person is practically independent of his/her actions or consent. In conditions of non-transparency of data processing, the unlimited possibility of obtaining such data using the “myth of consent” means consent to profiling, on the one hand, and consent to fragmentation of the digital self, on the other hand.¹⁰ Getting out of control and the sphere of human control, the elements of one’s identity become an object of appropriation, falsification, making a person more vulnerable. As a situation describing such vulnerability can be described the identity theft.

In particular, articles 4 and 7 of the Budapest Convention on cybercrime refer to the criminal legislation of the Member States in order to punish any violation that entails intentional and unlawful “damaging, deletion, deterioration, alteration or suppression of computer data without right”,¹¹ as well as deliberate and unauthorised “input, alteration, deletion, or suppression of computer data, resulting in inauthentic data with the intent that it be considered or acted upon for legal purposes as if it were authentic, regardless whether or not the data is directly readable and intelligible”.¹² Thus, the manipulation of personal data resulting from the theft of citizens’ personal data by entering another person’s personal digital data can damage a person’s physical and moral integrity. It should be noted that this position is also taken by the

⁹ EL-KHOURY, M., ARIKAN, C. L. From the internet of things toward the internet of bodies: Ethical and legal considerations. *Special Issue: Artificial intelligence in finance*. 2021, vol. 30, no. 3, pp. 307–314. [online]. Available at: <<https://onlinelibrary.wiley.com/doi/pdf/10.1002/jsc.2411>>.

¹⁰ See further VARDANYAN, L., STEHLÍK, V., KOCHARYAN, H. Digital Integrity: A Foundation for Digital Rights and the New Manifestation of Human Dignity. *TalTech Journal of European Studies*. 2022, vol. 12, no. 1, pp. 169–170.

¹¹ The Convention on Cybercrime (Budapest Convention, ETS No. 185) and its Protocols (Budapest, 23.XI.2001).

¹² Ibid.

ECtHR in the case of *K. U. v. Finland*.¹³ Fraudulent and malicious use of data related to a person's civil identity entails a change in his/her objective identity. Thus, the risks associated with the loss of control over digital identity can lead to the use of anonymity as a means of maintaining control over identity. P. De Hert analyses the need to recognise the "right to identity" in the light of the threats posed to humans by the IoT, defining profiling as the most important threat to identity, which creates new opportunities for manipulating people.¹⁴

Digital personal data, being a continuation of our existence in cyberspace, violates the basic principle of the human condition: the principle of immutability. The principle of immutability is becoming questionable due to digital identity, which is becoming increasingly subjective and changeable when using digital identification. On the other hand, the destruction of the principle of immutability becomes apparent when digital identification gets out of control due to changes made by humans and third parties. Thus, anonymity seems to be the only way to ensure control over a person who goes beyond what a person knows about himself/herself.

Moreover, the right to self-determination should include the freedom to transform one's digital identity, and it deserves explicit mention. This follows from the widespread right to consent to an intervention in one's body. This, in turn, presupposes the ability to allow other people to transform their bodies. Within this limited framework, the current law recognises "morphological freedom".¹⁵

It should be noted that the right to personal (bodily) integrity is complemented by other rights, especially human dignity. As the case law of the ECtHR shows, human dignity and the right to prevent degrading treatment can be applied to the retention or removal of assistive devices.¹⁶ Crucial to these ECtHR's judgments is the state of helplessness and dependence that people find themselves in. If removing wheels from a wheelchair by the police seems more undesirable than handcuffing a person, then the reason lies not in restricting movement (which may be the same in both cases), but in putting the person in an allegedly degrading state of helplessness and vulnerability. Dignity also protects the most important aspects of a person's attitude towards himself/herself. His/her field of activity includes prosthetics that restore a sense of personal (bodily) "integrity" (for example, the same wheels for the disabled). Nevertheless,

¹³ Case of *K.U. v. Finland* (Application no. 2872/02), Judgment, Strasbourg, 02 March 2009.

¹⁴ DE HERT, P. *A right to identity to face the Internet of Things*. Council of Europe Publishing [online]. Available at: https://cris.vub.be/ws/portalfiles/portal/43628821/pdh07_Unesco_identity_internet_of_things.pdf

¹⁵ BUBLITZ, C. The body of law: boundaries, extensions, and the human right to physical integrity in the biotechnical age. *The Journal of Law and the Biosciences*. 2022, vol. 9, no. 1. doi: 10.1093/jlb/lisac032.

¹⁶ See: HESELHAUS, S., HEMSLEY, R. Human Dignity and the European Convention on Human Rights. In: Becchi, P., Mathis, K. (eds.). *Handbook of Human Dignity in Europe*. Cham: Springer, 2019.

we should also understand that such cases cannot apply to all auxiliary devices, and certain boundaries should exist.¹⁷

The analysis of digital identity demonstrates that it is a rather complex and multifaceted phenomenon that combines objective and subjective aspects of personality. Digital identity, being an interpretation of a real person in cyberspace, creates both opportunities and threats for the individual himself/herself. On the one hand, it serves as a tool for protecting and expressing oneself, on the other hand, it becomes vulnerable to manipulation and abuse, such as identity theft and profiling. In the context of digital transformation, the principle of immutability of personality is under threat, which requires a revision of approaches to the legal protection of digital identity. Modern challenges, including the development of the IoT and IoB, contribute to an increase in the risks of loss of control over digital personal data.

Thus, it is necessary to recognise and protect the right to identity in the digital space, including protection from unlawful interference, the right to anonymity and the possibility of transforming one's digital identity. In this context, it is also necessary to develop comprehensive legal mechanisms that take into account the principles of consent, transparency and self-government in relation to digital identity. Besides, it is also necessary to develop effective tools for managing digital footprints taking into account the possible risks associated with digital profiling.

3. Informational self-determination as the basis for the right to digital identity?

Information technologies have given the person himself/herself the opportunity to project his/her own images in the digital space that reveal elements of a person's personality. Creating or choosing one's own content for one's digital identification involves providing the "digital person" (*homo digitalis*) with legal tools with which one can create and defend his/her choice. S. Benn highlights that if a person is confident that he/she can be himself/herself, he/she can believe in himself/herself as a person, so we can say that the law should provide a person with confidence that he/she can be who he/she wants to be. In this framework, a person is a subject who recognises himself/herself as an agent who chooses and tries to control his/her own course in the digital world.¹⁸ At the same time, the new informational nature of identification depends on data processing and information management. Therefore, many legal

¹⁷ BUBLITZ, C. The body of law: boundaries, extensions, and the human right to physical integrity in the biotechnical age. *The Journal of Law and the Biosciences*. 2022, vol. 9, no. 1. doi: 10.1093/jlbb/lzab032.

¹⁸ BENN, S. I. Privacy, freedom, and respect for persons. In: Schoeman, Ferdinand David (ed.). *Philosophical Dimensions of Privacy: An Anthology*. Cambridge: Cambridge University Press, 1984, pp. 223–244.

mechanisms that are provided and applied in the context of personal data protection can become legal instruments for protecting human identity.

However, the modern paradigm of personal data protection cannot fully ensure the protection of the individual in the digital world. For such fundamental protection, the legal doctrine proposes to justify the protection of personal data by the right to personal identity. In particular, N. de Andrade considers the right to personal identity as a right that covers, controls and protects a number of different types of information related to our personal identity or its components (digital, genetic, neural).¹⁹ The researcher defines the right to personal identity as the right to be different from others, to be unique.²⁰ The right to identity is presented and developed as a right regulating a number of shifts and transformations of identity between different ontological levels of “being” (possible – real; actual – virtual). Thus, the right to identity is the right to register the attributes of one’s personality (real → possible), as well as the right to recognition and identification (possible → real) in accordance with these defining characteristics. This right also includes the right to be presented the way one wants (virtual → real), that is, the right not to be misrepresented; the right to delete and recreate oneself anew (actual → virtual), an identity movement that includes the right to be forgotten (and, therefore, the right to start anew) and the right to multiple identities (virtual → real) – that is, the right to create, control and maintain different identities in a digital environment.²¹

P. Bernal, in turn, includes the following groups of rights as components of the “right to an online identity”: the right to create, assert, and protect that identity, as well as the right to control the connections between an online identity and the real person behind it. The researcher argues that the rights that form the right to identity should function as principles from which legal rights and norms can then be derived.²²

It should be noted that P. Bernal and N. de Andrade also consider the right to be forgotten as one of the fundamental legal instruments directly arising from the right to online identity. It is this right that makes it possible to choose information and data as the “building blocks” that will form his/her digital identity, to choose what information about him/her is and will be available, as well as to maintain and control

¹⁹ DE ANDRADE, N. N. G. Oblivion: The Right to Be Different from Oneself – Reproposing the Right to Be Forgotten (February 1, 2012). VII International Conference on Internet, Law & Politics. Net Neutrality and other challenges for the future of the Internet. *IDP: Revista de Internet, Derecho y Política*. 2012, no. 13, pp. 122–137; See also: DE ANDRADE, N. N. G. Right to Personal Identity: The Challenges of Ambient Intelligence and the Need for a New Legal Conceptualization. In: Gutwirth, Serge et. al. (eds.). *Computers, Privacy and Data Protection: An Element of Choice*. Springer, 2011, pp. 65–97.

²⁰ *Ibid.*

²¹ ANDRADE, N. N. G. D., FÊTEIRA, L. T., CUNHA, M. V. D. A. (eds.). *New Technologies and Human Rights: Challenges to Regulation*. London: Routledge, 2013.

²² BERNAL, P. A. The Right to Online Identity. *SSRN Electronic Journal* [online]. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2143138

what will belong to his/her reputation and dignity. From the above-mentioned point of view, the right of each person to create his/her own perimeter of digital identification may become a new perspective on the recognition of the right to digital identity as the basis of information self-determination. In particular, the GDPR states that individuals should have control over their personal data, and lays the foundation for recognising the right to information self-determination, the content of which can be determined using the rights provided for in the GDPR, i. e. the rights to receive information, deletion, correction, access, objection, restriction of processing, and data portability are not subject to a decision based solely on automated processing. We believe that recognising an individual's digital identity as a fundamental right will mean laying a new foundation for the rights provided for in the GDPR.

Moreover, even in its judicial practice, the CJEU considers the right to be forgotten as a certain emphasis on the assumption of the possibility of “managing” a digital person.²³ The judgment in the *Google Spain* case, as well as all subsequent judgments related to the right to be forgotten, grants a person the right to remove a link from search engines, giving a person a tool that allows them to control his/her digital identity.²⁴ Thus, anyone can create and develop his/her digital projection in the digital world by requesting the removal of a search engine index that is considered inadequate. Consequently, the right to be forgotten is becoming one of the tools for the formation of digital identity as the basis of information self-determination.²⁵ We believe that considering the right to be forgotten in this way can expand the scope of its application, becoming a so-called paradigmatic shift from the justification of confidentiality to the justification of identity.

As C. Sullivan points out, unlike the right to privacy, deviations from the right to identity cannot be justified by considerations of public interest and can only occur in exceptional circumstances, therefore, the right to identity provides better protection than the right to privacy.²⁶ At the same time, P. de Hert emphasises the need to clearly distinguish the right to identity from the right to privacy. P. de Hert argues that these new developments can have an important impact on our understanding of identity and require a new balance of interests that requires moving beyond established rights and

²³ VARDANYAN, L., STEHLÍK, V., KOCHARYAN, H. Digital Integrity: A Foundation for Digital Rights and the New Manifestation of Human Dignity. *TalTech Journal of European Studies*. 2022, vol. 12, no. 1, pp. 159–185.

²⁴ Case C131/12 – Judgment of the Court (Grand Chamber), 13 May 2014. *Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González*. ECLI identifier: ECLI:EU:C:2014:317.

²⁵ KOCHARYAN, H., VARDANYAN, L. The Right to Be Forgotten as a Legal Instrument for Expanding Informational Self-Determination in the Digital Age? *Constitutional Discourse*, 2024 [online]. Available at: <https://constitutionaldiscourse.com/the-right-to-be-forgotten-as-a-legal-instrument-for-expanding-informational-self-determination-in-the-digital-age/>.

²⁶ SULLIVAN, C. Digital Identity – the Legal Person? *Computer Law and Security Review*. 2009, vol. 25, no. 3, pp. 227–236.

concepts such as privacy, freedom, autonomy, and discrimination.²⁷ We agree with the researcher, since the right to privacy protects personal information that is in the private sphere. It provides protection against the publication of this information and its removal from personal life. At the same time, the right to be forgotten is aimed at protecting against the dissemination of information that has already been published, which, due to certain circumstances, distorts the modern idea of a person, his/her current identity. Consequently, the expansion of the context of the right to identity strengthens the right to information self-determination.

Moreover, a large amount of personal data is contained in publications on social networks or on platforms such as YouTube. Such information is protected by the fact that it is processed solely for “journalistic purposes” and is not subject to GDPR. In particular, the GDPR restricts the right to be forgotten in cases where restrictions are permissible for “journalistic, artistic or literary expression, to protect public interests in the field of public health, or for historical, statistical or scientific research purposes”. However, if we consider the right to be forgotten in the context of the right to identity, such an exception may not work. If information can create a misconception about a person’s personality, that is, a discrepancy between the personality conveyed through outdated information and the one that the individual wants to represent now, there is a possibility of applying the right to be forgotten. Indeed, the right to be forgotten can turn into the right to represent a real personal identity, who a person is and whom he/she wants to represent in society.

Determining the details of one’s physical and social identity contributes to personal development, since an individual has the right to such information, and this is important because of its impact on personality formation. In this regard, our democratic society must ensure that we can participate in shaping our future identity, as well as be able to get rid of certain parts of our past. This emphasises respect for the free choice of information by each person. As N. de Andrade correctly points out, since real identity can prevail only when past identities are forgotten, the right to be forgotten can play an extremely important role, allowing an individual to reconstruct the narrative of identity with confidence that past identities will not undermine this process.²⁸

²⁷ DE HERT, P. *A right to identity to face the Internet of Things*. Strasbourg: Council of Europe Publishing, 2007, [online]. Available at: https://cris.vub.be/ws/portalfiles/portal/43628821/pdh07_Unesco_identity_internet_of_things.pdf

²⁸ DE ANDRADE, N. N. G. Oblivion: The Right to Be Different from Oneself – Reproposing the Right to Be Forgotten (February 1, 2012). VII International Conference on Internet, Law & Politics. Net Neutrality and other challenges for the future of the Internet, *IDP. Revista de Internet, Derecho y Política*. 2012, no. 13, pp. 122–137; See also: DE ANDRADE, N. N. G. Right to Personal Identity: The Challenges of Ambient Intelligence and the Need for a New Legal Conceptualization. In: Gutwirth, Serge et. al. (eds.). *Computers, Privacy and Data Protection: An Element of Choice*. Springer, 2011, pp. 65–97; see also KOCHARYAN, H., VARDANYAN, L. The Right to Be Forgotten as a Legal Instrument for Expanding Informational Self-Determination in the Digital Age? *Constitutional Discourse*, 2024 [online]. Available at: <https://constitutionaldiscourse.com/the-rig>

The right to information self-determination can be considered as a mechanism of formation, one of the ways of which is to write a personal narrative that includes both the past and the future self of a person.²⁹ The link between one set of events and another, presented in our personal narrative, is the feeling of free will.³⁰ What made us us is usually explained by the choices we made. It is important to note that the reconciliation of the narrative is achieved by bringing one's behavior in line with the projected self-image. Control over the data that a person considers his/her personal narrative means the formation of his/her identity, and the right to information self-determination is based on a person's ability to choose and prioritize information about himself/herself.

It should be noted that the judicial practice of the ECtHR also deduces the right to identity from the interpretation of Article 8 of the ECHR. Thus, in the case of *Tysiack v. Poland*,³¹ the ECtHR confirmed that "private life" is a broad term covering, among other things, aspects of physical and social identity, including the right to personal autonomy, personal development, as well as to establish and develop relationships with other people and the outside world. Moreover, the ECtHR highlights not only the negative, but also the positive aspect of the right to respect for private life, in particular by including the right to develop one's personality within the framework of the right under consideration: such a personality develops not only "on its own", but also in our relationships with other people and the outside world. According to C. Sullivan, the ECtHR's position on personal identity is based on understanding the latter as a narrative, a continuous process of creating and recreating one's own life story.³² In turn, N. Tirosh argues that this right is neither a violation of the right to freedom of expression nor a guarantee of privacy, but rather the right to create their own narrative, appealing to the fact that people are given more "right of control" over their own personal data and, consequently, their identity.³³ We argue that modern threats to the individual in the digital world can be eliminated by introducing a right closely related to the ability to rethink oneself, form and present one's true identity to the world.

The doctrine points to the existence of *idem* and *ipse* identities.³⁴ In particular, *idem* identity corresponds to an outsider's view of a person, which considers personality

ht-to-be-forgotten-as-a-legal-instrument-for-expanding-informational-self-determination-in-the-digital-age/.

²⁹ VAN DER SLOOT, B. The right to be let alone by oneself: narrative and identity in a data-driven environment. *Law, Innovation and Technology*. 2021, vol. 13, no. 1, pp. 223–255. <https://doi.org/10.1080/17579961.2021.1898315>

³⁰ Ibid.

³¹ *Tysiack v. Poland*, Appl. No. 5410/03, Council of Europe: European Court of Human Rights, 20 March 2007.

³² SULLIVAN, C. Digital Identity – the Legal Person? *Computer Law and Security Review*. 2009, vol. 25, no. 3, pp. 227–236.

³³ TIROSH, N. 'Reconsidering the "Right to Be Forgotten" – Memory Rights and the Right to Memory in the New Media Era. *Media, Culture & Society*. 2017, vol. 39, no. 5, pp. 644–660.

³⁴ GLAS, G. Idem, Ipse, and Loss of the Self. *Philosophy, Psychiatry, & Psychology*. 2003, vol. 10, no. 4, pp. 347–352. <https://dx.doi.org/10.1353/ppp.2004.0018>; See also: FLORENCE

as the sum of stable characteristics. At the same time, the *ipse* identity corresponds to an individual as he/she relates to himself/herself. We note that the GDPR regulates the use of *idem* identification elements, a set of characteristics that identify a person, while *ipse* identity is only indirectly affected. From the point of view of *ipse* identity, the mechanisms specified in the GDPR cannot be considered effective, since they do not help a person present himself/herself to others the way he/she wants, however, we tend to believe that the right to information self-determination can potentially become mechanisms for protecting such identity. It is self-determination that aims to ensure the protection of identity formation and preservation: something that cannot be done in the modern paradigm of privacy and the legal paradigm in general, which do not allow it to adequately address emerging issues.

The same fundamental importance of self-determination for the formation of identity is also noted by the CJEU's case law, where self-determination is an element of the right to personal identity. In particular, AG Stix-Hackl, in his opinion on the *Omega* case, discussed the importance of human dignity and self-determination in shaping an individual's identity.³⁵ In general, human dignity has its roots deep in the origins of the concept of humanity in European culture, which views human as a being capable of spontaneity and self-determination. Because of his/her ability to form his/her own free will, he/she is a person and should not be reduced to the level of a thing or an object.³⁶ Thus, information self-determination as a mechanism for ensuring identity should have the potential to prevent the commodification of an individual through his/her personal data.

However, currently, on the one hand, there is legislative inflation, which is an indicator of the legal instability of the norm designed to ensure data protection, and, on the other hand, there is a violation of personal integrity due to the absence of a body in the digital space, where everything is done using digital personal data. According to Judith A. Howard, a person has as many identities as the social groups in which they manifest themselves and with which they enter into relationships.³⁷ Nothing else than the ability to "stay the same" introduces us to a temporal dimension in the sense that the ability to "stay" necessarily refers to the duration in time. One of the first conditions that allow a sense of identity to develop and "persist" is the stability of "civic identity", which is preserved over time. The ability to change one's personal data on the site or revoke consent, as well as numerous platforms with fake or outdated user profiles, disrupt this stability of civic identity, which remains suspended in

GIESBRECHT, D. Identities and prejudice: an essay from the thought of Paul Ricoeur. *ARIES, Anuario de Antropología Iberoamericana*, 2023. [online]. Available at: <https://aries.aibr.org/articulo/2023/01/4736/identities-and-prejudice-an-essay-from-the-thought-of-paul-ricoeur>

³⁵ Opinion of Advocate General Stix-Hackl delivered on 18 March 2004 [online]. Available at: <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:62002CC0036>

³⁶ Ibid.

³⁷ HOWARD, J. A. Social Psychology of Identities. *Annual Review of Sociology*. 2000, vol. 26, pp. 367–393.

the virtual world. At the same time, a significant part of human activity is currently dematerialised in cyberspace. The absence of bodies in cyberspace leads to the fact that an individual is easily replaced by his/her digital personal data, which leads to the destruction of the category of space and time in digital format. Under these conditions, it is no longer possible to talk about the stability of civic identity.

Nevertheless, digital identity is becoming an integral part of a human personal identity, and modern legal regulation based on the protection of personal data does not fully protect it. The right to identity, as an expanded concept, encompasses the control and protection of various aspects of digital identity, including the right to be forgotten, the right to multiple identities, and the right to self-actualisation in a digital environment. This right implies not only the protection of privacy and confidentiality, but also the management of one's own reputation and data, which contributes to the information self-determination of the individual. Thus, the expansion of the concept of the right to identity requires a new legal approach that ensures a balance between privacy, freedom and self-expression.

4. New approaches to our digital future

Catherine D'Ignazio and Lauren Klein point out that if we want to make our data-driven systems more humane, we will need to value multiple forms of knowledge, including those that come from humans as living, sentient bodies in the world.³⁸ Researchers highlight that the world of data often seems to us to be something cold, rational, objective and neutral, while in the “arena of machines and facts” there is no place for feelings and emotions. But humans, according to the researchers, are not just “two eyeballs attached by stalks to a brain computer”.³⁹ They are multisensory beings with culture, memories, fears, and feelings that are mostly lived, processed, and transmitted through their bodies. Nevertheless, we believe that this approach does not yet include the protection of enhancement devices, since their absence or damage does not deprive a person of the possibility of normal functioning. However, with the development of technology, as H. Stelarc correctly noted: “We are no longer just biological bodies. Rather, the body became a chimera, a combination of meat, metal, and code. The body has evolved into a hybrid and augmented operating system operating outside the skin.”⁴⁰

As one can see, the human body is being reinterpreted as an object for redesign, as a platform for activities in the world that can take different forms and connect to a variety of devices; as an open entity that transcends skin or biological physicality.

³⁸ D'IGNAZIO, C. & KLEIN, L. F. *Data Feminism*. Cambridge, Massachusetts, London: The MIT Press, 2020. <https://doi.org/10.7551/mitpress/11805.001.0001>

³⁹ Ibid.

⁴⁰ DONNARUMMA, M. ‘Fractal Flesh’, alternate anatomical architectures: An interview with Stelarc. eContact! 2005 [online]. Available at: https://econtact.ca/14_2/donnarumma_stelarc.html>

However, the question is, how far can such extensions extend in the context of legal protection? Perhaps the definitions of body boundaries should move to functional representations of the body as an “ensemble of intertwined functions”.⁴¹

The extended body thesis states that if an artifact contributes to normal functioning, it can be a part of the body and should be treated as such, provided that the person and the artifact can interact reliably and continuously. Such an expanded concept of the body, although indirectly, already leads to one conclusion: there must be individual powers that will help create this “ensemble”. Theoretically, such an opportunity is provided by the formulation of the provision enshrining the right to personal integrity in Article 3 of the CFR. Although the authors of the commentary on the CFR point out that the vision of human dignity underlining the prohibitions in Article 3(2) does not intend to promote individual rights, nevertheless, the widespread right to consent to interference in one’s body presupposes the ability to allow other people to transform their bodies.⁴² What third parties can do with a person’s permission, the person himself/herself should also be allowed (unless, of course, this requires special medical training). In this limited sense, the CFR theoretically recognises “morphological freedom”.⁴³ Thus, it is a right that ensures not only inviolability, but also self-determination.

A similar approach can be seen in the concept of bodily integrity, confirmed by the Supreme Court of the United States (Union, 1891), which ruled that no right is considered more sacred or more carefully protected by common law than the right of every person to own and control his personality, free from any restrictions or interference, other than on the basis of the clear and indisputable authority of the law.⁴⁴ In this judgment, personal (bodily) integrity is defined simultaneously as positive and negative freedom – as self-determination and integrity. Bodily self-determination presupposes that people should have the freedom to manage and control their bodies, whereas personal (bodily) integrity presupposes that people have the right to be free from unwanted coercion or influence.

As one can see, there is an expansion of the interpretation of the sphere of the right to personal integrity, which already does not coincide with the concept of the body, which is proved by the judicial practice of the ECtHR. However, today this design

⁴¹ CARTER, A., PALERMOS, S. O. Is Having Your Computer Compromised a Personal Assault? The Ethics of Extended Cognition. *Journal of the American Philosophical Association*. 2016, vol. 2, no. 4, pp. 542–560.

⁴² SCHABAS, W. *The European Convention on Human Rights: A commentary*, Oxford: Oxford University Press, p. 370.

⁴³ BUBLITZ, C. The body of law: boundaries, extensions, and the human right to physical integrity in the biotechnical age. *The Journal of Law and the Biosciences*. 2022, vol. 9, no. 1. doi: 10.1093/jlb/Isac032.

⁴⁴ WEILER, S. Bodily Integrity: A Substantiv Bodily Integrity: A Substantive Due Process Right to Be Free from Rape by Public Officials. *California Western Law Review*. 1998, vol. 34, no. 2, pp. 591–610. Available at: <https://scholarlycommons.law.cwsl.edu/cgi/viewcontent.cgi?article=1277&context=cwlr>

does not include a transhumanistic interest in enhancement devices. Damage to them remains damage to property, since it does not deprive a person of the possibility of normal functioning.

At the same time, as already noted, the GDPR recognises the general concept of personal data, but does not protect the internal relationship between personal data and identification. As Urgessa notes, “the current EU data protection regime protects information that relates to us, but, strictly speaking, does not protect ourselves”.⁴⁵ Thus, it can be said that this right provides an autonomous mode of using “personal data” without communicating with a person. Rather, the GDPR regulates the use of identification elements – a subjective measurement of a person, including his/her habits or preferences, for which data is often processed. In other words, the GDPR does not proceed from the fact that personal data (or part of it) is a projection of personality. Meanwhile, personal data is an integral part of personal identity, since there is no difference between a person’s information sphere, interpreted by these internal personal data, and his/her personal identity.⁴⁶ At the same time, the use of this data as a kind of personality projection requires more reliable and fundamental protection than that which can be achieved within the framework of the right to personal data protection. The existing legal protection of information identity is insufficient and does not cover a wide range of personal hazards.

From the point of view of legal mechanisms, this is possible with such rights, some of which are specified in the GDPR, for example, through the right to be forgotten. The GDPR, through its broad definition of personal data, also indicates that EU legislation recognises that personal data contributes to a person’s composite identity, although it does not directly mention the concept of “personal identity”. We believe that this will allow EU legislation to ensure the necessary protection of data that contributes to a person’s personal identity.

5. Conclusion

This analysis of digital identity highlights its deep complexity and the multifaceted legal challenges associated with its protection. However, the existing legal framework has difficulty providing adequate protection, as digital identity remains vulnerable to manipulation, unauthorised use, and opaque profiling mechanisms.

The right to informational self-determination must be recognised as a fundamental mechanism for managing and safeguarding digital identity. This requires ensuring

⁴⁵ URGESSA, W. G. The Feasibility of Applying EU Data Protection Law to Biological Materials: Challenging ‘Data’ as Exclusively Informational. *Journal of Intellectual Property, Information Technology and Electronic Commerce Law*. 2016, vol. 7, no. 2. DOI:10.2139/ssrn.2840764

⁴⁶ FLORIDI, L. The Ontological Interpretation of Informational Privacy. *Ethics and Information Technology*. 2005, vol. 7, 185–200. <https://doi.org/10.1007/s10676-006-0001-7>

robust protection against unlawful interference, maintaining the right to anonymity, and empowering individuals to shape and transform their digital presence.

The development of legal tools for digital identity management must align with principles of consent, transparency, and self-governance articulated by contemporary privacy scholars. Zuboff's critical analysis underscores the urgent need to resist the commodification of personal data and protect individual agency.⁴⁷ As digital identity continues to evolve, the recognition of individual control over personal digital footprints becomes essential in ensuring both personal autonomy and security in an increasingly networked environment.

In the context of digital transformation, a person exists not only as a biological entity, but also as a digital personality consisting of many fragments of data. However, the modern right to personal data protection is focused on information, not on protecting the individual himself/herself. This leads to a loss of control over digital identity and makes a person vulnerable to manipulation, profiling and digital fragmentation. The introduction of the right to information self-determination as an independent protection mechanism will allow a person not only to manage his/her data, but also to form an integral digital identity reflecting his/her real personality.

List of references

- ANDRADE, N. N. G. D., FÉTEIRA, L.T., CUNHA, M. V. D. A. (eds.). *New Technologies and Human Rights: Challenges to Regulation*. London: Routledge, 2013.
- BENN, S. I. Privacy, freedom, and respect for persons. In: SCHOEMAN, Ferdinand David (ed.). *Philosophical Dimensions of Privacy: An Anthology*. Cambridge: Cambridge University Press, 1984, pp. 223–244.
- BERNAL, P. A. The Right to Online Identity. *SSRN Electronic Journal* [online]. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2143138
- BUBLITZ, C. The body of law: boundaries, extensions, and the human right to physical integrity in the biotechnical age. *The Journal of Law and the Biosciences*. 2022, vol. 9, no. 1. doi: 10.1093/jlb/lsac032.
- CARTER, A., PALERMOS, S. O. Is Having Your Computer Compromised a Personal Assault? The Ethics of Extended Cognition. *Journal of the American Philosophical Association*. 2016, vol. 2, no. 4. pp. 542–560.
- D'IGNAZIO, C., KLEIN, L. F. *Data Feminism*. Cambridge, Massachusetts, London: The MIT Press, 2020. <https://doi.org/10.7551/mitpress/11805.001.0001>
- DE ANDRADE, N. N. G. Oblivion: The Right to Be Different from Oneself – Reproposing the Right to Be Forgotten (February 1, 2012). VII International Conference on Internet, Law & Politics. Net Neutrality and other challenges for the future of the Internet, *IDP. Revista de Internet, Derecho y Política*. 2012, no. 13, pp. 122–137.

⁴⁷ ZUBOFF, S. *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*. London: Profile Books, 2019.

- DE ANDRADE, N. N. G. Right to Personal Identity: The Challenges of Ambient Intelligence and the Need for a New Legal Conceptualization. In: GUTWIRTH, Serge et. al. (eds.). *Computers, Privacy and Data Protection: An Element of Choice*. Springer, 2011, pp. 65–97.
- DE HERT, P. *A right to identity to face the Internet of Things*. Strasbourg: Council of Europe Publishing, 2007 [online]. Available at: https://cris.vub.be/ws/portalfiles/portal/43628821/pdh07_Unesco_identity_internet_of_things.pdf
- DONNARUMMA, M. ‘Fractal Flesh’, alternate anatomical architectures: An interview with Stelarc. eContact! 2005 [online]. Available at: https://econtact.ca/14_2/donnarumma_stelarc.html
- EL-KHOURY, M. & ARIKAN, C.L. From the internet of things toward the internet of bodies: Ethical and legal considerations. *Special Issue: Artificial intelligence in finance*. 2021, vol. 30, no. 3, pp. 307–314 [online]. Available at: <https://onlinelibrary.wiley.com/doi/pdf/10.1002/jsc.2411>
- ELLIOTT, A. (ed.). *The Routledge Social Science Handbook of AI*. London: Routledge, 2021.
- FLORENCE GIESBRECHT, D. Identities and prejudice: an essay from the thought of Paul Ricoeur. *ARIES, Anuario de Antropología Iberoamericana*, 2023 [online]- Available at: <https://aries.aibr.org/articulo/2023/01/4736/identities-and-prejudice-an-essay-from-the-thought-of-paul-ricoeur>
- FLORIDI, L. *The Fourth Revolution: How the Infosphere is Reshaping Human Reality*. Oxford: Oxford University Press, 2014.
- FLORIDI, L. The Ontological Interpretation of Informational Privacy. *Ethics and Information Technology*. 2005, vol. 7, 185–200. <https://doi.org/10.1007/s10676-006-0001-7>
- GLAS, G. Idem, Ipse, and Loss of the Self. *Philosophy, Psychiatry, & Psychology*. 2003, vol. 10, no. 4, pp. 347–352. <https://dx.doi.org/10.1353/ppp.2004.0018>
- HESELHAUS, S., HEMSLEY, R. Human Dignity and the European Convention on Human Rights. In: BECCHI, P., MATHIS, K. (eds.). *Handbook of Human Dignity in Europe*. Springer, Cham, 2019.
- HOWARD, J. A. Social Psychology of Identities. *Annual Review of Sociology*. 2000, vol. 26, pp. 367–393.
- KOCHARYAN, H., VARDANYAN, L. The Right to Be Forgotten as a Legal Instrument for Expanding Informational Self-Determination in the Digital Age? *Constitutional Discourse*. 2024 [online]. Available at: <https://constitutionaldiscourse.com/the-right-to-be-forgotten-as-a-legal-instrument-for-expanding-informational-self-determination-in-the-digital-age/>.
- NISSENBAUM, H. *Privacy in Context: Technology, Policy, and the Integrity of Social Life*. Stanford: Stanford University Press, 2010.
- ROBLES-CARRILLO, M. Digital identity: an approach to its nature, concept, and functionalities, *International Journal of Law and Information Technology*. 2024, vol. 32, no. 1.
- RODRIGUES, R. E. Revisiting the legal regulation of digital identity in the light of global implementation and local difference. The University of Edinburgh, Dissertation collection, 2011, p. 55 [online]. Available at: <https://era.ed.ac.uk/handle/1842/8942>
- SCHABAS, W. *The European Convention on Human Rights: A commentary*. Oxford: Oxford University Press, p. 370.
- SULLIVAN, C. Digital Identity – the Legal Person? *Computer Law and Security Review*. 2009, vol. 25, no. 3, pp. 227–236.

- TIROSH, N. 'Reconsidering the "Right to Be Forgotten" – Memory Rights and the Right to Memory in the New Media Era. *Media, Culture & Society*. 2017, vol. 39, no. 5, pp. 644–660.
- URGESSA, W. G. The Feasibility of Applying EU Data Protection Law to Biological Materials: Challenging 'Data' as Exclusively Informational. *Journal of Intellectual Property, Information Technology and Electronic Commerce Law*. 2016, vol. 7, no. 2. DOI:10.2139/ssrn.2840764
- VAN DER SLOOT, B. The right to be let alone by oneself: narrative and identity in a data-driven environment. *Law, Innovation and Technology*. 2021, vol. 13, no. 1, pp. 223–255. <https://doi.org/10.1080/17579961.2021.1898315>
- VARDANYAN, L., STEHLÍK, V., KOCHARYAN, H. Digital Integrity: A Foundation for Digital Rights and the New Manifestation of Human Dignity. *TalTech Journal of European Studies*. 2022, vol. 12, no. 1, pp. 159–185.
- WEILER, S. Bodily Integrity: A Substantiv Bodily Integrity: A Substantive Due Process Right to Be Free from Rape by Public Officials. *California Western Law Review*. 1998, vol. 34, no. 2, pp. 591–610. Available at: <https://scholarlycommons.law.cwsl.edu/cgi/viewcontent.cgi?article=1277&context=cwlr>
- ZACCARONI, G. Fundamental rights and disruptive technologies: a right to personal identity under the European multi-level system of protection? *Freedom, Security & Justice: European Legal Studies*. 2020, no. 3, pp. (155) 143–166. DOI: 10.26321/G.ZACCARONI.03.2020.06
- ZUBOFF, S. *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*. London: Profile Books, 2019.