



Volume 11 Issue 1



RESEARCH
ARTICLE



OPEN
ACCESS



PEER
REVIEWED

Legal boundaries of digital identity creation

Ewa Michalkiewicz-Kadziela *University of Szczecin*
Ewa Milczarek *University of Szczecin*

DOI: <https://doi.org/10.14763/2022.1.1614>

Published: 14 January 2022

Received: 16 March 2021 **Accepted:** 10 June 2021

Competing Interests: The author has declared that no competing interests exist that have influenced the text.

Licence: This is an open-access article distributed under the terms of the Creative Commons Attribution 3.0 License (Germany) which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited. <https://creativecommons.org/licenses/by/3.0/de/deed.en>
Copyright remains with the author(s).

Citation: Michalkiewicz-Kadziela, E. & Milczarek, E. (2022). Legal boundaries of digital identity creation. *Internet Policy Review*, 11(1). <https://doi.org/10.14763/2022.1.1614>

Keywords: Identity, Human rights, Digital identity, EU law, Avatars

Abstract: The internet has created possibilities to define human identity in a digital world. This entails the need to consider the impact of this new environment of identity's operation and the effects of possible differences. The authors analyse digital identity in terms of its relation with human identity derived from Article 8 of the Convention for the Protection of Human Rights and Fundamental Freedoms. The paper's research goal is to specify the relation between digital identity and real identity, aiming in essence to provide an answer to the following research question: does the internet as the new sphere of identity's operation have such an effect that it created a need to specify a legal framework and methods of protection unique to digital identity? This study aims to specify legal tools for creating digital identity and the legal boundaries of the possible creation.

1. Introduction

Technological progress has a great impact on many spheres of social and economic life. Although this impact is largely positive, as it brings people new solutions that improve their comfort of living (e.g. treatment of thus far untreatable conditions or easy access to information), we still cannot forget that along with the emergence of innovative technologies, there are new areas that are not covered by relevant regulation. Such a situation often results from the lack of adequate legal tools that could be applied in such cases. Such issues are most often solved by adequate application of laws in force and by the creation of new laws that address this problem.

The emergence of a universally accessible internet undoubtedly has been one of the greatest technological achievements of the last five decades. However, although it presented numerous benefits, it also brought a catalogue of issues that had not been regulated thus far. Digital identity is unquestionably one of such issues.

Human identity itself and its legal regulation cause many problems, especially since human identity is a complex phenomenon. From the point of view of the state, human identity is a set of objective features that allow the citizen to be identified. From the point of view of the individual, human identity entails both objective and subjective features that she herself creates and through which she expresses herself. Therefore, it should not be surprising that it is not easy to find the golden mean that ensures security of the state and the freedom of citizens' expression. Moreover, the emergence of the internet caused the creation of one's identity to move to the virtual world. New tools of creation were set up, which thus far had existed in the 'real world', e.g. social networking sites, business portals or search engines. As a result, we can create a digital identity which is linked with our real identity. Less often, such digital identity will only function in the virtual world (e.g. an avatar).

In this context, the aim of the article is to establish the relation between digital identity and real identity, which in essence means an intention to answer the following research questions: what is the standard-setting role of the law in protecting the individual's fundamental right to identity in the digital age? Are threats to online identity new and unique? If yes, can existing laws that regulate real identity be applied to digital identity or must new laws be created that will regulate such issues individually?

In order to be able to answer the research questions, on the one hand we use research methods typical in legal studies and on the other hand we make reference to the achievements in social sciences (mainly sociology and psychology) combined with IT knowledge. As a result, our research material includes legislative acts, judicial decisions and relevant literature in legal, social sciences and IT scholarship. The research focuses mainly on European international law, with particular emphasis on the European Convention on Human Rights (hereinafter: ECHR), which has become an anchor for the regulation of human identity in regional international law, and also European Union law—which has recently focused strongly on regulating matters associated with new legal issues of the virtual world.

2. The right to human identity

The terms human identity and digital identity must be explained if we are to correctly qualify the relation between them. The first should be understood as a relatively new human right which was derived from the interpretation of Article 8(1) of the ECHR: *Everyone has the right to respect for his private and family life, his home and his correspondence*. However, it has already established itself in the arena of international law and has also been accepted into the canon of European Union regulations (see the introduction of the Charter of Fundamental Rights of the European Union), which means that it may be considered a universal law.

The European Court of Human Rights (hereinafter: ECtHR), in an array of judgments pertaining to the right to privacy, came to a conclusion that this right has a broader scope than thus far believed. The body of judicial decisions has determined that the right to privacy also covers the complex concept of human identity.

The right to identity has not been comprehensively addressed in a single ruling of the European Court of Human Rights, but its various elements can be interpreted from a combination of judgments. First of all, we assume that the right to identity protects such elements of identity as name, surname, right to know one's origin, gender or ethnicity (*Godelli v. Italy*, 2013; , *Mikulić v. Croatia*, 2002; *Odièvre v. France*, 2003). However, it should be noted that this catalogue is only one illustration. Over the years, the content of the right to identity has developed, thanks to which other elements of human identity, such as image, citizenship (*Relu Adrian Coman and Others v Inspectoratul General pentru Imigrări and Ministerul Afacerilor Internet*, 2018), voice or pseudonym (Sieńczyło-Chlabicz, 2006, p. 151) have also been protected by human rights law. Moreover, it is worth noting that the content of the right to identity is constantly evolving, and thus new elements of human identity are being incorporated into the protection of this right, e.g. freedom of dress, sexu-

al identity or internet identity.

Some elements of identity are objective, allowing identification of a specific person (for example name, surname, date of birth). However, most other elements are subjective, which means that they can be shaped by ourselves.

Until recently, the creation of one's identity, composed of subjective elements, took place in the real world, thanks to how we presented ourselves to other people and how the people around us perceived us. However, currently the opportunity to create one's own identity has also moved to the internet, and the interpretation of Article 8 of the ECHR is a standard for other laws in the system of European legislation that regulates these issues.

3. Impact of the digital environment on human identity

The internet is reshaping our perception of the world around us and of ourselves. It is an important element of social communication today. These arguments are based on an underlying assumption that the creation of human identity online runs differently, especially given the fact that in the virtual world we might have new tools of creation at hand that are unavailable in the real world.

The specific characteristics of the virtual environment have a substantial impact on building individual elements of identity on the internet. Cyberspace is defined by information, data and connections between these data (Starrs, Anderson, 1998 p. 148). Cyberspace as a sociosphere (Sienkiewicz, 2015, pp. 89-95) is used to implement social processes, including revealing the identity (Bernd, 2006, p. 1021). Elias Aboujaoude shows its effects on people's behaviour and changes in terms of identity-building. The internet affects all aspects of everyday life, the boundary between what is virtual and what is real disappears, and in its place there is a vacuum with uncertain rules and an almost complete lack of restrictions, and an alienated state of existence (virtualism) (Aboujaoude, 2011). "A web act", despite the same assumptions and the same intention (*finis operantis*) as a "real" act, often has a different outcome (*finis operis*). This is largely associated with a different moral assessment of the same act on the internet and in (analogue) reality. This is mainly determined by the fact that the environment—cyberspace—is an abstract thing for the user, and thus outcomes of his actions seem not real to him (it should be noticed that some virtual activities lead to real/tangible outcomes) (Wyrostkiewicz, 2015, p. 7). As a consequence, we need to point out that the behaviour of internet users, including the shaping of identity on-line, will be different than would be the case in the 'real world'.

Social Self Theory created by George Herbert Mead (Mead, 2015) is grounded on an assumption that people build their identity based on the perspective that the self emerges from social interactions, such as observing and interacting with others, responding to others' opinions about oneself, and internalising external opinions and internal feelings about oneself.

Analysing individual elements of identity building derived by Mead, we point out that in cyberspace:

- there is a different way of entering into and conducting social interactions;
- observation of others and image creation is done by other tools, for example search engines, social profiles;
- there is increased freedom in expressing opinions.

This leads to the conclusion that the digital environment indeed affects the forming of human identity causing it to be modifiable in a different way than the real identity. This is not only because different tools of creation are used, but also because cyberspace is attractive and gives an illusory impression of a lack of supervision over the content posted on-line. The possibilities of creating an identity detached from the real identity are especially attractive for social media users where this identity is based not on a real person, but on a nickname, an avatar (e.g. on Instagram, TikTok, on-line games, etc.). These platforms do not require users to provide their actual identification data, unlike, for example, Facebook or LinkedIn, where providing such information is mandatory. The sense of unrestricted freedom and new tools contribute to the difference in the formation of human identity on the internet. Giving some thought to the influence of the internet on human identity allows us to formulate a hypothesis that the digital human identity is so different from the real identity that it constitutes a new research subject. This leads to a need to examine how digital identity differs from human identity created by a person in the 'real world'.

4. Digital human identity

Digital identity can be described as a set of data that uniquely describes a person or a thing and contains information about its connections (Windley, 2005, p. 8; Sullivan & Stalla-Bourdillon, 2015, p. 268). Given the above we must conclude that digital identity means a set of external elements—data, left in cyberspace, which make up a vision of one's own personality and one's attributes.

The sum of digital traces makes it possible to specify a given entity's created image, consumer behaviour, preferences and interests (by means of relevant web-

sites) as well as written or declarative traces which directly reflect ideas and opinions (Ertzscheid, 2016).

When analysing the functioning of digital identities, we can identify digital identity proper (relating to the material substrate—that is a real person) and independent (occurring only in a virtual, non-physical world). Identity in the digital world is built in a non-material environment, based only on data supplied by users. The author of the information decides whether he associates the information provided by him with his real person, whether he leaves it anonymous or whether he associates it with the entity created by him only on-line (a frequent occurrence in virtual worlds). This increases the individual's creation-related possibilities.

In the first case, creation of digital identity is built on the basis of the identity of the “real” person. In this situation, digital identity will be part of the “real” identity and will be homogeneous in nature. Both identities interact with each other. This situation prevails in most cases. Digital identity proper includes an identity used in eID systems of a profile on social networks when acting under one's own surname, such as Facebook, LinkedIn, etc.

In the second case, digital identity is built only in the digital environment. It will be created in the language strata (messages and other digital traces). In such situations, the individual uses a nickname or login instead of their personal details. In this case, the digital identity does not coincide with the real identity and they are independent of each other. Independence in this case can be very strong, when the user in the virtual world creates an identity based on different characteristics than in the case of real identity, for example indicating a different skin colour, profession, experience, origin or sexual preferences. If the overall situation of the interaction is not related to structural constraints, or when these constraints are ambiguous—as in cyberspace, individuals will have more freedom to choose their identities and are more likely to activate more than one identity (Styker & Burke, 2000).

Some creators recognise digital identity as an extended version of real social identity (Wojno, 2010, p. 64).

Similar to identity in the ‘real world’, digital identity will be built on the basis of objective and subjective elements.

Human identity means objective features, independent of the human, and subjective features, created by her with certain limitations. These are mainly external

features (e.g. image), objective identifying features (e.g. genetic code), subjective mental features (e.g. gender), features resulting from social formation that were approved by the individual and with which she identifies (e.g. medical doctor, lawyer). Proper digital identity will consist of the following categories of data:

1. Data identifying a person and connecting them to a real identity such as name and surname (objective element).
2. Data indirectly identifying a person like username, login, email address, IP address, nickname, alias (subjective element).
3. User-dependent data creation: photographs, logos, content placed on social networks (Facebook, Instagram, LinkedIn and others) (subjective element).
4. User-independent data creation: digital traces, data about a person placed by other network users such as press articles, posts (subjective element).

Objective elements will occur only in the case of proper digital identity and constitute the first of the above.

Digital identity will be forged mainly through messages created by a user and those about a user (created by other actors). The impression made is controlled through digital identity management (Windley, 2005).

5. Legal boundaries for the protection of digital identity

Tools designed to guarantee protection of an individual's broadly understood privacy, are often related to protection of elements of human identity. However, these tools should be read in a multidimensional way—that is, not only as a protection measure, but also as a creative tool. Most of the tools available on the internet allow information to be removed at the request of the person concerned. This means that a user himself may decide which information should be available to third persons, which consequently affects his image created on the internet. For example, on the one hand, the right to be forgotten allows users to protect their privacy (by being able to remove information that violates this privacy). On the other hand, it allows users to remove information inconsistent with the identity created by them (e.g. by deleting information published before gender reassignment). Tools for the protection of the right to privacy are created in various ways. Internet service providers (ISPs) may produce them at their own initiative, but most often it is legal obligations that impose that such tools should be put in place. The legislative activity of the European Union and the CJEU's decisions are prominent in this regard.

Regarding the law functioning at the level of the European Union, the most comprehensive protection of identity is provided by provisions covering the protection of personal data. They are subject to extensive legal protection, included in several legal acts. However, the most important of them is the Regulation on the protection of personal data (hereinafter referred to as: GDPR), which is a universally binding act, and therefore, as it may seem, the most effective.

This efficiency mostly results from the fact that this regulation by operation of law automatically becomes part of the member states' national law. This means that when it comes to protection of personal data, the European Union states are obliged to apply uniform regulations.

The personal data enumerated in these guidelines can also act as elements of identity. Therefore, it is the identity related not only to basic elements that allow an individual to be identified, but also with such elements that the person can create herself. What is more, it is not only the real identity that is subject to GDPR provisions, but these provisions can also refer to identity functioning in the virtual world.

The CJEU has set forth relevant digital identity protection tools mainly through preliminary rulings issued as a response to questions referred to by national courts of member states. It must be emphasised that these tools are unique to the digital environment and cannot be applied to other jurisdictions. They include: the right to be forgotten (*Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González*, 2014; Article 17 GDPR) and the preventive blocking of unlawful content on social networks (*Glawischnig-Piesczek v Facebook Ireland Limited*, 2019). If one were to analyse these tools jointly, it may be evidenced that protection of digital identity is based on the possibility of removing unwanted information from internet sites, social media and search engines. The scope of application of these tools is broad. First and foremost, the user has the right to request that unlawful or offensive information about him or information that is not consistent with the facts or outdated be removed. Such a request may be restricted due to access to information issues, for instance.

However, legal boundaries of creating digital identity have their limits and relevant criteria for their potential application. One of the basic criteria for specifying those boundaries is the status of a private or public person (privacy of public figures is protected in a narrower scope than the privacy of other persons) (*von Hannover v. Germany* (no. 2), 2012; *Oberschlick v. Austria* (no. 2), 1997). The second criterion refers to information: private or professional (§29 and §43 *Niemietz v. Ger-*

many, 1992). The third criterion refers to materiality of information in a democratic society (*von Hannover v. Germany* no. 2, 2012) (e.g. associated with freedom of expression and information, courts' exercising justice, public health, scholarly or historical research or statistical purposes).

When specifying legal boundaries for creating digital identity one should each and every time decide what the purpose of a certain category of information relevant to an individual is. Therefore, since the right to identity is derived from dignity and the right to privacy (Michalkiewicz-Kadziela, 2020), without a doubt all restrictions on its creation must be implemented according to Article 8 ECHR.

Legal tools for protection of digital identity are not harmonised on the international level, which results from the fact that in different countries we are dealing with a different interpretation of the content of the right to privacy and the right to protection of personal data—which are the source of creation of laws that regulate issues pertaining to the protection of digital identity in Europe. This is caused not only by belonging to separate legal systems, but also by being part of separate legal cultures that have a different axiological basis. It is worth noting that what the United States call “personally identifiable information” (PII) is a fundamentally different legal entity than “personal data”, a term used in EU data protection laws, although they are both essential components of digital identity in their respective jurisdictions (Holt & Malčić, 2015, p. 158). As emphasised by Sullivan and Stalla-Bourdillon, “civil law personality rights, such as those recognised in France and in other jurisdictions which have inherited French legal concepts, fit better with the nature and functions of digital identity. These rights can readily apply to recognise and protect an individual’s rights and interests in his/her assigned digital identity [...]” (Sullivan & Stalla-Bourdillon, 2015, p. 268). However, we can clearly see that the tools described above, provided for in the EU legal order, are put to work in other systems too, as seen in the case of the right to be forgotten—a feature universally available on Google.

Tools for protection of digital identity may only be applied to protection of digital identity proper. Independent digital identity, if not associated with real identity, is not subject to protection as the actor using it does not have a legal personality. However, one must ponder whether independent digital identity should be covered by legal protection. This is because it involves the right to remain anonymous.

The ECtHR has recognised the importance of anonymity to the rights to freedom of expression and privacy (European Court of Human Rights, 2011, p. 48). As indicated by the Polish Supreme Court, “the username used by a person on a website is

subject to legal protection on the basis on which the name, nickname or company is protected” (Judgment of the Polish Supreme Court, 2008). The social and economic importance of aliases is increasing. Creations, which are present exclusively on the internet, are becoming more frequent. If they allow identification of a given user identity, they should undoubtedly be protected. This should apply not only to cases where the nickname can be linked to a natural person, but also where the real identity of the person is unknown. The protection of anonymity is an important element of protecting both the right to freedom of expression and the right to privacy (e.g. in Universal Declaration of Human Rights and International Covenant on Civil and Political Rights). As Clare Sullivan states, “the right to identity, as an international fundamental human right, should now be recognized and protected in relation to digital identity” (Sullivan, 2016, p. 474). This postulate would be difficult to materialise due to the issue of specifying legal and judicial capacity of an anonymous actor. However, it may successfully function through recognition by internet services, which may process requests filed by users to protect their proper self-sovereign identity (analogically, as in the case of the right to be forgotten).

7. Conclusions

Without a doubt the essence of human identity is the same, regardless of the sphere of its exercise. However, human identity on the internet functions on completely different terms than outside it. The internet gives unlimited possibilities of creating subjective elements of one’s own identity, but it also allows a change of objective elements.

Differences between identity on the internet and outside it are significant enough to necessitate separate research. The internet impacts the functioning of identity to such a degree that it implicates the need to specify a legal framework and methods of protection unique to digital identity.

On the one hand, new technologies pose a threat to the protection of the right to identity, but on the other hand, if skilfully used, they can be a tool for its implementation. In the case of a proper digital identity, its creation cannot take place in any way that allows a person to shape an image in a digital world that deviates from the real one, misleads or hides some information. Therefore, shaping digital identity will not be subject to full freedom, and will be limited by legal boundaries.

Legal boundaries of protection of identity of a person will be most visible in the question of counteracting unwanted messages. As pointed out above, an individual

has the right to have information relating to her removed in order to create a desired image on the web within the limits stipulated by legislation and the related case-law.

Digital identity without a doubt will gain significance both in the question of e-ID and in the social and economic dimension. Independent digital identity at the moment does not have a significant role, though its growing participation in the digital life created the need to regulate methods of its protection.

References

Aboujaoude, E. (2012). *Virtually you: The dangerous powers of the e-personality* (Norton paperback). Norton.

Bernd, M. (2006). Personality in Cyberspace: Personal Web Sites as Media for Personality Expressions and Impressions. *Journal of Personality and Social Psychology*, 90(6), 1014–1031. <https://doi.org/10.1037/0022-3514.90.6.1014>

Charter of Fundamental Rights of the European Union, Pub. L. No. C 326/391 (2012).

Convention for the Protection of Human Rights and Fundamental Freedoms (European Convention on Human Rights). (1950). Council of Europe. https://www.echr.coe.int/documents/convention_eng.pdf

Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ L 119 27.04.2016 (2016). <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016R0679>

Ertzscheid, O. (2016). *What is digital identity? Issues, tools, methodologies*. OpenEdition press.

Eva Glawischnig-Piesczek v. Facebook Ireland Limited, C.-18/18 (Opinion of Advocate General Szpunar June 4, 2019). <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62018CC0018>

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

Google Spain SL and Google Inc. V. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González, Case C-131/12 (Audiencia Nacional May 13, 2014). <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62012CJ0131>

Holt, J., & Malčić, S. (2015). The Privacy Ecosystem: Regulating Digital Identity in the United States and European Union. *Journal of Information Policy*, 5, 155–178. <https://doi.org/10.5325/jinfopoli.5.2015.0155>

Judgment of the Polish Supreme Court of 11 March 2008, CSK 539/07 (Polish Supreme Court March 11, 2008). <https://sip.lex.pl/orzeczenia-i-pisma-urzedowe/orzeczenia-sadow/ii-csk-539-07-wyrok-sadu-najwyzszego-520502124>

Mead, G. H. (2015). *Mind, self, and society* (The definitive edition). University of Chicago Press.

Michałkiewicz-Kądziela, E. (2020). *Prawo do tożsamości człowieka w prawie polskim i międzynarodowym*. Wydawnictwo C.H. Beck.

Mikulić v. Croatia, Application no. 53176/99 (European Court of Human Rights February 7, 2002). http://www.aimjf.org/storage/www.aimjf.org/Jurisprudence_CEDU/CASE_OF_MIKULIC_v._CROATIA.pdf

Niemietz v. Germany, Application no. 13710/88 (European Court of Human Rights December 16, 1992). <https://hudoc.echr.coe.int/eng?i=001-57887>

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

Relu Adrian Coman and Others v. Inspectoratul General pentru Imigrări and Ministerul Afacerilor Internet, Case C-673/16 (Grand Chamber June 5, 2018). <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62016CJ0673>

Research Division. (2011). *Internet: Case-law of the European Court of Human Rights* [Report]. Council of Europe. https://www.echr.coe.int/documents/research_report_internet_eng.pdf

Sieńczyło-Chlabicz, J. (2006). *Naruszenie Prywatności Osób Publicznych Przez Prasę*. Zakamycze. <https://sip.lex.pl/komentarze-i-publicacje/monografie/naruszenie-prywatnosci-osob-publicznych-przez-prase-analiza-369150921>

Sienkiewicz, P. (2015). Ontologia cyberprzestrzeni. *Zeszyty Naukowe WWSI*, 13(9),

89–102.

Starrs, P. F., & Anderson, J. (1997). The Words of Cyberspace. *The Geographical Review*, 87(2), 146–154. <https://doi.org/10.2307/216002>

Styker, S., & Burke, P. J. (2000). The Past, Present, and Future of an Identity Theory. *Social Psychology Quarterly*, 63(4), 284–297. <https://doi.org/10.2307/2695840>

Sullivan, C. (2016). Digital Citizenship and the Right to Digital Identity under International Law. *Computer Law & Security Rev*, 32(3), 474–481. <https://doi.org/10.1016/j.clsr.2016.02.001>

Sullivan, C., & Stalla-Bourdillon, S. (2015). Digital Identity and French Personality Rights – A Way Forward in Recognising and Protecting an Individual's Rights in His/Her Digital Identity. *Computer Law & Security Review*, 31(2), 268–279. <https://doi.org/10.1016/j.clsr.2015.01.002>

Universal Declaration of Human Rights (UDHR), General Assembly resolution 217 A (1948). <https://www.un.org/sites/un2.un.org/files/udhr.pdf>

International Covenant on Civil and Political Rights, (1966). <https://www.ohchr.org/en/professionalinterest/pages/ccpr.aspx>

Von Hannover v. Germany, Application no. 59320/00 (European Court of Human Rights June 24, 2009). <https://hudoc.echr.coe.int/fre?i=001-61853>

Windley, P. J. (2005). *Digital identity* (1st ed). O'Reilly.

Wojno, A. (2010). "Ja" w Cyberprzestrzeni. *Opieka, Wychowanie, Terapia*, 3–4(64), 59–64.

Wyrostkiewicz, M. (2015). *Internet i (nie)moralnosc*. Wydawca MW Press.

Published by



ALEXANDER VON HUMBOLDT
INSTITUTE FOR INTERNET
AND SOCIETY

in cooperation with



CREATE



centre
— internet
et **societe**



R&I
IN3
Internet
interdisciplinary
Institute
Universitat Oberta de Catalunya



UNIVERSITY OF TARTU
Johan Skytte Institute of
Political Studies