Bulletin of the *Transilvania* University of Braşov
Series VII: Social Sciences • Law • Vol. 18(67) Special Issue – 2025
https://doi.org/10.31926/but.ssl.2025.18.67.3.26

# POST-MORTEM DATA PROTECTION IN THE DIGITAL AGE: A NECESSITY FOR HUMAN DIGNITY?

**Yann I. CONTI**[1]

***Abstract:*** *The rise of digital society raises new questions about the status of the digital remains of deceased individuals. Recent literature argues that such remains require protection similar to that afforded to bodily remains, due to their connection to personal identity. By framing post-mortem privacy as an essential component of human dignity, we show that protecting the digital remains of the deceased is necessary both to uphold informational self-determination and to ensure respect for the person beyond death. Drawing on recent developments in the domestic laws of several EU Member States, we argue that data protection law provides a particularly suitable framework for safeguarding human dignity in relation to digital remains. The issue is timely, as it is currently under consideration within the European "Digital Decade" policy programme.*

***Key words:*** *data protection, Post-Mortem privacy, human dignity, right to self-determination*

## 1. Introduction

The rise of digital society raises pressing questions about the privacy of deceased individuals, whose digital data in most cases remains online. European data protection law has so far focused on living persons, leaving Member States free to decide whether to regulate post-mortem data protection – with uneven uptake.

This paper explores post-mortem privacy as a matter of human dignity. It first reviews how recent literature defines post-mortem privacy and its relation to dignity (2). It then analyses national data protection regimes across Member States from a comparative perspective, highlighting emerging trends (3). Finally, the study assesses how these regimes safeguard dignity through the idea of post-mortem privacy and concludes with recommendations for strengthening the EU framework to better protect human dignity in relation to the deceased (4).

[1] *University of Zurich*, yann.conti@uzh.ch. This contribution is the author's own independent initiative, and his opinion does not represent that of any institutions to which he may be affiliated.

## 2. Extending the Dignity of the Deceased: The Role of Post-Mortem Privacy

This article argues that post-mortem privacy can – and should – be seen as a novel extension of the dignity of the deceased. The exploitation of one's digital data after death should be controllable in a similar manner as bodily remains are to be protected against unwanted manipulations or commercialization after death.

To this end, we will first examine how the fate of bodily remains is linked to protecting the dignity of the deceased (2.1), then address the issue of privacy protection in relation to digital remains (2.2).

### 2.1. Dignity of the deceased: The case of bodily remains

There is a long-standing idea that the dignity of the deceased must be protected beyond death. A clear illustration is the treatment of bodily remains, which must respect the dignity of the deceased.

The protection of dignity is a supreme right of the individual. It appears in Article 1 of both the Universal Declaration of Human Rights and the EU Charter of Fundamental Rights. The protection of human dignity derives from the Kantian philosophy: "*So act that you use humanity, whether in your own person or in the person of any other, always at the same time as an end, never merely as a means*" (Kant, 1997, p. 38, [4:429]). This view of human dignity is implemented in the previously mentioned international treaties but also at the national level in Western jurisdictions. As a matter of example, dignity heads the list of fundamental rights in the German Constitution in Article 1 (1): "*Die Würde des Menschen ist unantastbar. Sie zu achten und zu schützen ist Verpflichtung aller staatlichen Gewalt*".

What is true for the living individual is also true to a certain extent for the deceased. Even after death, human dignity commands that some respect is due to the deceased. The idea that the protection of human dignity extends beyond an individual's biological lifetime once again finds its source in Kant's philosophy, according to which each individual is entitled to assert the defense of the reputation of the deceased (*bona fama defuncti*) (Kant, 1996, p. 76, [6:295] f.).

This philosophy has long since found its way into civilian systems. The principles of modern private law generally aim to safeguard the human dignity of the deceased. One of the main emanations of this idea is the right of a person to decide what happens with their bodily remains and have these wishes honored. In Germany the concept of *Totenfürsorge* constitutes a personal, non-patrimonial right to decide how a deceased person is buried and how their body is handled (Muscheler, p. 349). This institution is primarily rooted in the constitutional guarantee of human dignity (Art. 1 of the German Constitution) and the general personality protection enshrined by case law (NJW 1954 1404, p. 1405). If the deceased has expressed wishes regarding burial, these prevail; if not, the close relatives are both entitled and obliged to decide on the disposition of the body and to determine the type and place of the burial (NJW-RR 1989 1159, p. 1160).

In Italy, the equivalent institution is the *ius sepulchri* (right of burial), a personal right recognized by case law. According to this principle, every individual is free to choose the

terms and location of their burial (*ius eligendi sepulcrum*). In the absence of an expressed wish by the deceased, the decision rests with the close relatives (known as the family *ius sepulchri*). Similar institutions are well established in other jurisdictions, such as Austria, France or Switzerland.

From a conceptual point of view, these institutions illustrate what we will refer to as the "protection of the bodily remains" in private law. This notion encompasses two elements. This notion encompasses two elements. On the one hand, the intention of the deceased should prevail over the rights of close relatives; the right of disposition over bodily remains thus constitutes an extension of personal autonomy beyond death. On the other hand, where no instructions have been left, close relatives are under a duty to handle the bodily remains in a manner respectful of the deceased – that is, an obligation on the part of the survivors to treat the deceased with dignity. The underlying idea is that the right to determine one's post-mortem treatment is an extension of personal dignity and autonomy, persisting beyond death and balancing individual will with family and societal duties.

### 2.2. Post-Mortem privacy: The Case of digital remains

In the wake of the development of information technology and the digitalization of society, the question arises as to whether the principles governing the protection of bodily remains should also, in some form, apply to digital remains. The parallel is based on the idea that post-mortem privacy would be an integral part of human dignity (2.2.1), while digital remains should be understood as a new form of bodily remains in digital form (2.2.2).

#### 2.2.1. *Post-Mortem Privacy as an Extension of the Protection of the Dignity of the Deceased*

At the outset, it should be emphasized that the European conception of the right to privacy is rooted in the protection of human dignity (Whitman, 2003, p. 11). The right to privacy allows a person to control what others know about them and to decide what and how they want to reveal personal information. It prevents third parties from instrumentalizing individuals through the unauthorized collection or processing of their data (the primary aim of data protection) and safeguards the individual's capacity for self-determination and self-realization (the core concern of personality protection). As the Italian philosopher Luciano Floridi (2016, p. 308) argues: "*Privacy should be grafted as a first-order branch to the trunk of human dignity, not to some of its branches, as if it were a second-order right*". Human dignity is thus the normative root of privacy rights.

Yet, while dignity extends beyond death, the same is not as true for privacy. In principle, privacy protection ends upon the death of the individual, either by virtue of the adage "*actio personalis moritur cum persona*" in common law systems, or due to the extinction of personality rights in civil law systems (Stilinović, 2023, p. 213 ff). In most cases, indirect protection remains when an infringement upon the deceased simultaneously affects the honor of the surviving relatives. These considerations are obviously subject to punctual exceptions depending on the jurisdiction and sectorial

practices. This means that privacy after death is generally not recognized as a right of the deceased themselves, but rather as a derivative protection grounded in the dignity of the person and the interests of the living. In this context, there is a growing sense of a legal vacuum in the digital environment, where personal data do not disappear upon death but continue to circulate, be stored and exploited.

It is precisely this gap that has given rise to the notion of post-mortem privacy in legal scholarship, particularly in connection with the broader issue of digital inheritance (Buitelaar 2017, p. 129 ff; Edwards and Harbinja, 2013, p. 101 ss; Davey, 2020, p. 13 ff). Post-mortem privacy has thus emerged as a corrective measure to the loss of control that individuals experience upon death over their personal information saved online in the hands of third parties in the form of digital data (Edwards and Harbinja, p. 135 ff). It aims to extend the individual's ability to preserve the protection of their privacy beyond death, as this protection is increasingly threatened by the technological revolution.

The first sophisticated and authoritative definition of post-mortem privacy is that of Edwards & Harbinja, who formulated it in 2013 as "*the right of a person to preserve and control what becomes of his or her reputation, dignity, integrity, secrets or memory after death*" (Edwards & Harbinja, 2013, p. 103). Later, Harbinja (2020, p. 91) refined the definition, by stating that post-mortem privacy is "*the right of the deceased to control his personal digital remains post-mortem, broadly, or the right to data protection post-mortem, narrowly defined*". Her concept rests on the principle of autonomy, which should transcend death in the same way that testamentary freedom allows post-mortem control of property.

Several other significant contributions further enrich this discussion. Buitelaar advances the theory that the digital double of the deceased should be afforded "*an appropriate locus in the legal framework that governs the survival or extinction of the rights and duties of subjects*" (Buitelaar, 2017, 131 ff). His argument builds upon the notion of an informational self, suggesting that the privacy rights of this digital double should be regarded as a continuation of the ante-mortem individual's privacy rights, thereby compensating for the absence of a living counterpart (Buitelaar, 2017, p. 139).

In 2020, Davey proposed that the privacy right enshrined in Art. 8 of the ECHR should be extended beyond death and be conceived as "*the right of a person to respect for her private and family life post-mortem*". Central to her argument is the notion of "post-mortem relational privacy", according to which the privacy interests of the living are intimately connected to those of the deceased. Surviving relatives may suffer harm when private or intimate information about a deceased person is disclosed (Davey 2020, p. 183 ff.). Importantly, actual disclosure is not required for harm to occur; the mere risk of posthumous revelation may already infringe upon the privacy interests of the living (Davey 2020, p. 127).

We can therefore identify distinct normative grounds underpinning the same institution: the transcendence of a person's autonomy beyond death, on the one hand, and the protection of living persons as justification for the protection of the deceased, on the other.

The general idea that post-mortem privacy is an aspect of human dignity has been empirically confirmed by Harbinja, Morse & Edwards (2025, p. 11). In their survey, 80%

of the 1766 respondents answered that they "strongly agree" or "somewhat agree" to the affirmation "privacy is an aspect of human dignity".

These developments reveal a growing consensus that the protection of privacy must evolve to address the online persistence of personal identity in the form of digital data. Rooted in the concept of human dignity, post-mortem privacy thus emerges as a conceptual bridge between the autonomy of the deceased and the emotional integrity of the living.

#### 2.2.2. *Digital remains: Should they be afforded protection comparable to bodily remains?*

We now turn to whether digital remains should be afforded comparable protection to bodily remains based on the protection of post-mortem privacy. For this purpose, we first have to define what "digital remains" are – or mean. Öhman defines them as "*any* [*digital*] *data we leave behind: Facebook profiles, Spotify playlists and preferences, Google search histories, Zoom logs, emails, video games avatars, chat logs, photo libraries, and so on*" (Öhman, 2024, p. 48). This definition reflects the general idea that everyone leaves digital footprints online, which persist in the absence of any deliberate action to remove them.

Öhman and Floridi (2018, p. 319; 2017, p. 649 ff.) link digital remains to personal identity in much the same way as bodily remains are tied to the deceased individual. They argue that everyone leaves, besides bodily remains, an informational corpse – or informational body – after death (Öhman and Floridi, 2018, p. 319; 2017, p. 647; Floridi, 2014, p. 122). An informational corpse is an "[i]*norganic body of a human constituted and existing through information related to his identity*" (Harbinja, 2020, p. 91; Floridi, 2014, p. 122). This corresponds to Floridi's standpoint that data are not possessions but rather constitutive elements of one's identity (Floridi, 2014, p. 122; Floridi, 2016, p. 308). Within this framework, individuals are information and their data constitute an extension of their own identity and body. Therefore, violating someone's informational privacy is not just a breach of ownership but an attack on the person's dignity and, by extension, on humanity itself (Floridi, 2016, p. 308; Ohman and Floridi, 2017, p. 647).

The analogy between bodily remains and digital remains gains depth when viewed through Stokes' distinction between "self" and "person" (Stokes, 2016, p. 211 ff.; 2015, p. 240). While death terminates the conscious "self", the "person" – understood as a narrative identity – may continue to persist. The role of digital remains and bodily remains is therefore similar in that they preserve the narrative identity of the deceased.

In line with that approach, Öhman & Floridi (2017, p. 649 f.) suggest that the commercial use of one's digital remains after their death consists in a manipulation of one's informational corpse. Echoing Kant's philosophy, they support that "*Ethically, human dignity requires that digital remains, seen as the informational corpse of the deceased, may not be used solely as a means to an end, such as profit, but regarded instead as an entity holding an inherent value*" (Öhman & Floridi, 2018, p. 319). These authors further affirm that digital remains should be protected from commercial use to the same extent as bodily remains are protected by the International Council of Museums (ICOM). The latter provides that bodily remains must be treated in accordance with their inviolable human dignity and that "*all aspects of the commercial venture*"

should be carried out with respect for "*the intrinsic value of the original object*" (Article 2.10 of the ICOM Code of Professional Ethics 1986).

The protection of digital remains can thus be conceived in a manner conceptually analogous to the protection of bodily remains. Because digital data continue to represent and project aspects of personal identity, a protection inspired by the preservation of human dignity beyond death appears fully justified. In the context of this contribution, we focus on how data protection can serve this purpose.

## 3. Emerging Trends in National Data Protection Regimes Across European Union Member States

Post-mortem control of digital remains can be achieved through a data protection regime. Data protection is particularly appropriate insofar as it concerns absolute subjective rights that can be exercised *erga omnes* against any data holder. We will see that emerging trends in the European Union Member States' domestic data protection regimes aim to achieve some of the objectives of post-mortem privacy. For the purposes of this analysis, we assume that most digital data generated online by an individual qualifies as personal data within the meaning of the GDPR, given that true anonymization is rarely achievable in practice (Conti/Schoenenberger, 2025, p. 82 fn. 72).

One peculiarity at the European Union level is that post-mortem data protection falls outside the scope of the GDPR. Recital 27 explicitly provides that "[*t]his Regulation does not apply to the personal data of deceased persons. Member States may provide for rules regarding the processing of personal data of deceased persons*".

Currently, ten of the twenty-seven Member States have taken the opportunity to incorporate rules on the protection of the personal data of deceased individuals into their national legislation, in varying scopes and degrees of detail. These are, in alphabetical order, Bulgaria, Denmark, Estonia, France, Hungary, Italy, Portugal, Slovakia, Slovenia and Spain. Interestingly, the analysis of these regimes reveals emerging trends towards implementing the two identified aspects of post-mortem privacy: the data subject (ante-mortem) right to self-determination beyond death, on the one hand, and the (post-mortem) intervention of surviving relatives in the management of personal data after death, on the other hand.

Some Member States have established in their data protection acts mechanisms that allow the data subject's wishes, expressed during their lifetime, to determine the post-mortem fate of their data protection rights – and thus of their personal information in the form of digital data that they leave behind. These Member States enshrine, to varying extents, a right to informational self-determination over personal data after death. In France, the French Data Protection Act allows any person to define directives (which are amendable or revocable at any time) relating to the storage, erasure, and communication of their personal data after their death (French Data Protection Act, Art. 85). These directives define how the data subject wishes that their right to data protection be exercised after their death. The data subject may designate a person responsible for their execution. In the same vein, Hungarian law (Section 25 Para. 1 of the Hungarian Data Protection Act) provides that the data subject may authorize a third

party to exercise the rights conferred by Articles 15 to 18 and 21 of the GDPR by means of a declaration made to the controller and incorporated in a private document having probative force. Other Member States have limited themselves to establishing mechanisms that allow the data subject to limit or to prohibit the post-mortem exercise of data protection rights by the survivors authorized by the law. A compelling example is Art. 2-*terdecies* Para. 2 of the Italian Data Protection Act which provides that "*the exercise of the* [data protection] *rights referred to in paragraph 1 is not permitted* […] *when, limited to the direct offer of information society services, the data subject has expressly prohibited it by means of a written statement submitted to or communicated to the data controller*". Portugal, Slovenia and Spain have similar provisions in their data protection acts.

A more common legislative practice across Member States is the allocation of post-mortem data protection rights to survivors (close relatives and/or heirs). The said allocation is differentiated from one Member State to another. Danish law provides that the GDPR shall apply to the data of deceased individuals for a period of 10 years following the death of the data subject (Art. 1 Para. 2 *lit*. 5 of the Danish Data Protection Act). Italy grants the rights set out in Articles 15 to 22 of the GDPR to the authorized survivors (Art. 2-*terdecies* Para. 1 of the Italian Data Protection Act), while Spanish law only mentions the rights of access, rectification and erasure (Art. 3 Para. 1 of the Spanish Data Protection Act). Portuguese law mentions the same rights as Spanish law, but the list does not appear to be exhaustive (Art. 17 of the Portuguese Data Protection Act). Bulgaria (Art. 25f Para. 2 of the Bulgarian Data Protection Act) and Slovenia (Art. 9 of the Slovenian Data Protection Act) limit the post-mortem prerogatives to a simple right of access and/or a right to obtain a copy of the deceased's personal data.

We can observe that these legislative practices result in a certain symmetry with the protection of bodily remains.

On the one hand, we find that some Member States recognize an ante-mortem prerogative, namely a "right of disposition of the digital remains", allowing individuals to determine during their lifetime the fate of their personal data after death. This mirrors the traditional right to decide on the treatment of one's bodily remains.

On the other hand, we observe a post-mortem prerogative, namely a "right of management of the digital remains" granted to survivors, rather than a duty comparable to the duty of disposition of bodily remains. This shift from a duty to a right is justified by the difference in scale between handling a single human corpse and managing the multitude of digital footprints accumulated during a lifetime. Such a task is undeniably daunting, which makes it more appropriate to conceive it as a right for survivors rather than an obligation. The corresponding duties could instead be imposed on data controllers by emerging legal frameworks, given their *de facto* exclusive technical control over the deceased's digital data. Such obligations might arise only where survivors choose to exercise their post-mortem rights; yet a more general obligation imposed directly on data controllers, independent of any action by survivors, also remains conceivable.

The emerging system that is already enshrined in some Member States' national law, albeit still fragmented and incomplete, opens up the possibility of a comprehensive system that could eventually be extended at the supranational level in the GDPR.

## 4. Towards a Stronger European Union Data Protection Framework

Our analysis is particularly timely since consideration of legislative action at supranational level regarding post-mortem data protection is currently on the European agenda. The recently launched "Digital Decade" of the European Union sets targets for Europe's digital transformation to ensure a human-centric, inclusive, and sustainable digital future, strengthening Europe's digital sovereignty.

In this context, the European Declaration on Digital Rights and Principles for the Digital Decade was published with the idea of promoting a digital transition shaped by European values. It enshrines a set of digital rights and principles that reflect the EU values. In a sub-chapter entitled "Privacy and individual control over data", Chapter V Para. 19 states that "*Everyone should be able to determine their digital legacy, and decide what happens with their personal accounts and information that concerns them after their death. We commit to: a) ensuring that everyone has effective control of their personal and non-personal data in line with EU data protection rules and relevant EU law; b) ensuring effectively the possibility for individuals to easily move their personal and non-personal data between different digital services in line with portability rights; c) effectively protecting communications from unauthorised third party access; d) prohibiting unlawful identification as well as unlawful retention of activity records*".

We observe that the general idea of post-mortem privacy protection is already reflected to a certain extent in the Declaration, namely that the individual should have an effective control of their data beyond death and they should have their electronic communications protected from unauthorized third-party access (on this topic, see Conti, 2025, p. 50 ff) and should not be subject to unlawful retention of activity records.

While the idea of self-determination already seems to permeate the text of the Declaration, the role of surviving heirs and/or close relatives regarding the management of the deceased's personal data is not expressly stated. It is in our opinion crucial that European law also tackles the right of the survivors to take – subsidiarily to the intention of the deceased – the necessary measures to ensure that the informational body left behind is handled with dignity. Leaving aside the situation in which the person did not determine what should happen with their online information would most likely create legal uncertainty at the European Union level (Șchiopu, 2023, p. 19).

Such a right of the survivors could be conceived as a data protection prerogative. In this context, the surviving person would be entrusted with data protection prerogatives enabling them to manage the fate of the digital data left online by the deceased and, therefore, to manage the information consisting of digital identity elements left by the deceased. The shift from a duty to a right that we have identified in the practices of the Member States provides a useful starting point for considering how to integrate, in a coherent manner, the difference in nature between bodily remains and digital remains. It thus offers an opportunity to establish a regime for the protection of an individual's digital remains that must be conceptualized in an innovative way in the digital context while at the same time fulfilling functions equivalent to those associated with the control of bodily remains.

## 5. Conclusion

Post-mortem privacy should be understood as a novel extension of the dignity of the deceased. Despite their material differences, digital remains should be handled after death in a way that is – to a certain extent – functionally similar to bodily remains, insofar as both sustain the post-mortem presence of the person.

In that respect, data protection is expected to play a crucial role as informational bodies are composed of digital data which are also personal information (regardless of whether data protection law formally classifies them as personal data). In the wake of the Digital Decade, European law is expected to develop a legal framework aiming at managing one's digital legacy. To this end, it will be necessary to guarantee the data subject's right to informational self-determination by giving them the possibility to control during their lifetime the fate of their personal data after death, thus giving effect to a binding will that would be enforceable on third parties. Moreover, it will be necessary to conceptualise the situation in which the deceased has not taken any decisions during their lifetime: it will then be up to the European law to designate close relatives and/or heirs as custodians of the deceased's digital remains and potentially involve data controllers in the process by imposing corresponding obligations on them.

In a rapidly evolving digital environment, where the effectiveness of traditional legal institutions is still in question, one may wonder whether data protection regulations are sufficient to protect the "intrinsic value" of digital remains. In any case, the establishment of a post-mortem data protection regime would be an essential first step towards better protection of the dignity of the deceased – and thus of the living.

## References

Buitelaar, J.C. (2017). Post-mortem privacy and informational self-determination. *Ethics and Information Technology,* 19, 129–142. https://doi.org/10.1007/s10676-017-9421-9.

Conti, Y. & Schoenenberger, Y. (2025). Implementation of Digital Data Erasure: an Interdisciplinary Perspective. *University of Vienna Law Review*, 9(3), 64–98, https://doi.org/10.25365/vlr-2025-9-3-64.

Conti, Y. (2025). Electronic Communications of Deceased Users: How European Law Can Help Strike a Balance Between Post-Mortem Access and Privacy. *European Data Protection Law Review*, 11(1), 50–59. https://doi.org/10.21552/edpl/2025/1/9.

Davey, T. (2020). *Until Death Do Us Part: Post-mortem Privacy Rights for the Ante-mortem Person*. Doctoral thesis, University of East Anglia. Retrieved from https://ueaeprints.uea.ac.uk/id/eprint/79742/.

Edwards, L. & Harbinja, E. (2013). Protecting Post-Mortem Privacy: Reconsidering the Privacy Interests of the Deceased in a Digital World. *Cardozo Arts & Entertainment Law Journal*, 31(1), 101–148.

Floridi, L. (2014). T*he fourth revolution: How the infosphere is reshaping human reality*. Oxford University Press.

Floridi, L. (2016). On Human Dignity as a Foundation for the Right to Privacy. *Philosophy*

*& Technology,* 29, 307–312. https://doi.org/10.1007/s13347-016-0220-8.

Harbinja, E. (2020). The 'New(ish)' Property, Informational Bodies, and Postmortality. In M. Savin-Baden, & V. Mason-Robbie (Eds.), *Digital Afterlife* (18 pages). Taylor & Francis.

Harbinja, E., Morse T. & Edwards L. (2025). Digital Remains and Post-mortem Privacy in the UK: What Do Users Want? *International Review of Law, Computers and Technology.* Advance online publication. https://doi.org/10.1080/13600869.2025.2506164.

Kant I. (1996) [1797]. *The Metaphysics of Morals*. Translated and edited by Mary Gregor. Cambridge University Press. Retrieved from https://archive.org/details/metaphysicsofmor0000kant.

Kant I. (1997) [1785]. *Groundwork of the Metaphysics of Morals*. Translated and edited by Mary Gregor. Cambridge University Press.

Muscheler K. (2024). *Das Recht des Todes, Grundlegung einer juristischen Thanatologie*. Duncker & Humboldt.

Öhman C. (2024). *The Afterlife of Data, What Happens to Your Information When You Die and Why You Should Care*. Chicago University Press.

Öhman, C. & Floridi, L. (2017). The Political Economy of Death in the Age of Information: A Critical Approach to the Digital Afterlife Industry. *Minds and Machines,* 27, 639–662. https://doi.org/10.1007/s11023-017-9445-2.

Öhman, C. & Floridi, L. (2018). An Ethical Framework for the Digital Afterlife Industry. *Nature Human Behaviour,* 2, 318-320: https://doi.org/10.1038/s41562-018-0342-4.

Șchiopu, S.-D. (2023). EU Regulatory Perspectives on Digital Legacy in View of the Respect Owed to the Dead: A Blessing for Individuals and a Curse for Businesses? *Law Review*, 13(2), 14–20. https://www.ceeol.com/search/article-detail?id=1210976.

Stilinović M. (2023). *Personality Rights and Inheritance – Is there such a Thing as Privacy after Death? Eu and Private International law: Trending Topics in Contracts, Successions and Civil Liability*. Editoriale Scientifica Napoli.

Stokes P. (2015). Deletion as second death: the moral status of digital remains. *Ethics and Information Technology*, 17, 237–248. https://doi.org/10.1007/s10676-015-9379-4.

Stokes P. (2016). Temporal Asymmetry and the Self/Person Split. *The Journal of Value Inquiry*, 51, 203–219 (2017). https://doi.org/10.1007/s10790-016-9563-8.

Whitman J. Q. (2003). *The Two Western Cultures of Privacy: Dignity Versus Liberty.* Available at SSRN*:* http://dx.doi.org/10.2139/ssrn.476041.