Teka Komisji Prawniczej PAN Oddział w Lublinie
vol. XIX, 2026, no. 1, pp. 153-165
https://doi.org/10.32084/tkp.10696

RIGHT TO BE FORGOTTEN IN THE DEEPFAKE ERA

Dr. Ewa Michałkiewicz-Kądziela

University of Szczecin, Poland
e-mail: ewa.michalkiewicz-kadziela@usz.edu.pl; https://orcid.org/0000-0002-5396-1820

Dr. habil. Wojciech Szczepan Staszewski

The John Paul II Catholic University of Lublin, Poland
e-mail: wojciech.staszewski@kul.pl; https://orcid.org/0000-0002-4139-3475

Abstract. Continuous technological development based on Artificial Intelligence is leading to the emergence of numerous new digital tools that impact human rights and may undermine the effectiveness of the mechanisms that currently protect them. In this publication, the authors decided to examine one of the human rights protection instruments, the right to be forgotten, regulated in the General Data Protection Regulation, and relate its operation to deepfake technology, which enables the creation of new content using AI models. The Authors' research goal was to examine the extent to which Article 17 of the GDPR, in its current form, can serve as an effective instrument for personal data protection in the face of the challenges posed by deepfake technology. In order to answer this question, they analyzed the adequacy of the contemporary understanding of the concept of personal data, the characteristics of deepfakes, and the effectiveness of the right to be forgotten in the context of the malicious use of deepfakes. Based on these considerations, the Authors concluded that the current model of the right to be forgotten is losing its effectiveness and requires redefinition. At the very end, the Authors propose a new legal approach to the protection of individuals and present the concept of transforming the right to erasure personal data into a broader right of an individual to control their digital identity.

Keywords: deepfakes; synthetic media; informational autonomy; right to be forgotten; digital identity; GDPR.

INTRODUCTION

The right to be forgotten has become a legal instrument available to individuals whose personal data has been used unlawfully, infringing personal rights, or whose use is harmful. More than a decade has passed since its interpretation by the Court of Justice of the European Union on 13 May 2013,

ISSN 1899-7694
e-ISSN 2719-7379

in the Google Spain case.[1] During this time, this right has not only evolved through further case law of the Court but also been established in legal provisions – article 17 of the EU General Data Protection Regulation (GDPR).[2] It is generally believed that the right to be forgotten has become an effective measure of protecting personal within the European Union [Cook 2015, 122], although it is not free of drawbacks, such as the lack of cross-border action or the lack of a remedy against decisions made by data controllers regarding the deletion of personal data. Currently, it is widely considered as one of the few tools, alongside the EU's Artificial Intelligence Act (AI Act),[3] that could become a remedy in the fight against the new challenge that deepfakes pose in EU law [Romero Moreno 2024, 297]. This unique technology, which uses someone's image, voice, or other individual characteristics, allows for the creation of realistic manipulated images and audio, causing a completely fictional event to be perceived as real and, as a result, may have a negative impact on the factual and legal situation of the person whose personal data was used to create deepfakes. The emergence of this technology and its widespread use makes it difficult, and sometimes even impossible, to determine whether a given recording is real or has been manipulated, which is why deepfakes enable such a strong connection between a given person and a fictional situation. Although deepfake technology itself is not a negative phenomenon, its malicious use may lead to serious violations of the law and restrictions on the protection of individual rights.

The rapid development of synthetic media, exemplified by deepfakes, has raised certain doubts about the sufficiency and adequacy of legal measures previously used to protect individuals from violations of their fundamental rights. Until now, the right to be forgotten has been considered a relatively efficient mechanism enabling individuals to independently shape their informational autonomy. Article 17 of the GDPR provided the ability to restore control over their personal data in the event of unauthorized use (e.g., through the right to rectification or erasure). However, deepfakes are a different story, as individuals lose influence over the false information

[1] Judgement of the Court of Justice of the European Union of 13 May 2013 – Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González, C-131/12.

[2] Regulation (EU) 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, L 119/1.

[3] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act)

disseminated about them, based on data that never existed, was never created, or was never shared.

The purpose of this publication is to examine the extent to which Article 17 of the GDPR can serve as an effective instrument for personal data protection in the face of the challenges posed by deepfake technology. This mechanism is quite distinct from other methods of generating and disseminating false information. This concerns not only the technical aspects of deepfake production (the use of AI tools and models, rapid replication), but also the form and origin of the data used in the process of creating manipulated audiovisual material. Due to the specific nature of deepfakes and their use of personal data, it is possible to formulate a hypothesis that Article 17 of the GDPR in current shape does not provide full and effective protection for individuals against personal data breaches, particularly due to the limited scope of this provision and the real practical difficulties associated with enforcing an individual's right to delete data from the digital environment. To verify this statement, it is necessary to determine the real scope of application of Article 17 of the GDPR with respect to generated deepfakes. Furthermore, can the data used by AI models to generate deepfakes be classified as personal data under the GDPR? Furthermore, to what extent does Article 17 of the GDPR allow for the removal of generated deepfakes from the digital world, and what are the actual and legal limitations associated with this?

1. ARTICLE 17 OF THE GENERAL DATA PROTECTION REGULATION

Originally, the right to be forgotten was not enshrined in law, but was a product of the case law of the Court of Justice of the European Union [Zhang, Finckenberg-Broman, Hoang, et al. 2025, 2447]. While the protection of personal data and the possibility of requesting the erasure of personal data had indeed existed before (e.g., Article 12(b) of Directive 95/46/EC[4]) [Klimas 2024, 105], the right to be forgotten was a new, comprehensive legal concept. Its regulation in Article 17 of the GDPR gave individuals tools to guarantee control over their personal data.

Under Article 4(1) of the GDPR, personal data means any information that allows for the direct or indirect identification of a natural person. For example, a personal identifier may include: a name, an identification number, location data, an online identifier, or one or more factors of the

[4] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, Official Journal L 281 , 23/11/1995 P. 0031 – 0050.

physical, physiological, genetic, mental, economic, cultural, or social identity of a natural person. This open list of identifiers makes the scope of personal data protection quite broad. At the same time, Article 17(1) of the GDPR provides a broad set of grounds for personal data protection in the digital sphere, although it should be remembered that it is closed in nature. A request made to the controller to have one's data deleted, which according to the definition in Article 4(1) of the GDPR may be considered personal data, may be made in several specific cases: the collection of the already gathered personal data is no longer necessary, the consent to the use of personal data is withdrawn, an objection to data processing has been filed, the data has been used unlawfully, the data must be deleted due to the necessity to comply with a legal obligation, the data has been collected in connection with the provision of information society services.

Article 17(2) of the GDPR, however, is quite important in ensuring the effectiveness of the right to be forgotten. It establishes the obligation of a controller who has made third-party data public to inform controllers processing that information that the data subject has requested that those controllers delete all links to, or copies or replications of, that personal data [Nasiadka 2023, 83-84]. In this way, the legislator has attempted to systematically restrict the dissemination of personal data that are to be forgotten at the request of the individual.

2. DEEPFAKES – CHARACTERISTICS

Deepfake technology has led to a qualitative change in the process of disseminating false information. It has radically increased its effectiveness, scale, and the difficulty of counteracting the negative consequences for individuals. From a practical perspective, deepfakes have become a more credible tool for disinformation than all other forms (e.g., fake news). This technology has created the ability to manipulate the recipient using image and sound, which is usually more convincing to the recipient than altered text or photo context [Ahmed and Chua 2023, 5]. This manipulation is facilitated by the ongoing development of technology making the created audiovisual materials increasingly difficult to identify, often leading to a lack of realistic opportunity to challenge fictitious content. Although the AI Act introduces the obligation to label deepfakes as content generated using artificial intelligence, the exemption from this obligation in certain cases must be taken into account and so must the lack of cross-border impact of this act outside the borders of the European Union. This means that the recipient will still be able to see manipulated materials without any information about their modification. The results of an investigation conducted by researchers from the University of Bristol (UK) are also disturbing, as they show that

the impact of deepfakes on humans is so strong that it exerts a manipulative influence on their perception, even when the content is marked as AI-generated [Clark and Lewandowsky 2026, 11].

Attention should also be paid to the increased accessibility of digital tools. Before the development of artificial intelligence, access to them was difficult not only due to their cost but also due to the requirement for technical skills on the part of the creator [Sivarajah, Heidemann, Lawrence, et al. 2022, 12]. This often required highly advanced technical knowledge [Pawelec and Łabuz 2025, 6]. Today, creating manipulated audiovisual materials is relatively inexpensive, and the ability to generate them using widely available AI tools and models means they can be created by anyone [Alanazi and Asif 2024, 51].

The widespread creation of AI-based content has made it possible to disseminate manipulated content in a very short time and on an unprecedented scale. This, however, leads to the extremely dangerous phenomenon of losing control over deepfakes after their publication. This content can not only be copied but also modified and republished in an altered version. The speed of multiplication is also crucial, allowing a deepfake to gain global reach in a matter of minutes [van der Sloot and Wagensveld 2022, 11]. This creates real difficulties, including identifying the entity to which a request for removal of digital content should be addressed, and, in the longer term, determining which individual data used to create subsequent versions of deepfakes can be classified as personal data, subject to GDPR protection.

3. EFFECTIVENESS OF THE RIGHT TO BE FORGOTTEN

The dynamic development of digital technologies is rendering traditional legal measures that have proven effective until now ineffective. One response to technological progress that eludes legal frameworks was the right to be forgotten, which was created as a tool for controlling personal data used online. With hindsight, the changing realities of how users operate online, and the growing amount of data processed by generative artificial intelligence models, we must question its current effectiveness and efficiency. Answering this question requires a multifaceted analysis, primarily addressing the impact deepfake technology has on the contemporary understanding of personal data, the possibility of its effective removal from the virtual world, and the independence in shaping one's information autonomy.

According to the definition of personal data contained in Article 4(1) of the GDPR, personal data are all elements that directly or indirectly enable the identification of a given person. Most of the data used by AI tools to create deepfakes does indeed utilize personal data in its traditional sense,

but sometimes this data is used to create other synthetic data. This leads to a blurring of the line between real data and data generated in the digital environment, which in turn makes it difficult to legally classify this data under the GDPR.

Without a doubt, personal data such as image, voice, or other individual characteristics used by AI models to generate deepfakes and relating to a specific natural person must be classified as personal data [Ruschemeier 2025, 4-5]. However, uncertainty arises when a deepfake creates a borderline situation – the generated material is not a faithful representation of a specific person, but uses certain characteristics (e.g., facial expressions) in such a way that the deepfake can be associated with that person. This raises the question: does a certain resemblance to a real person enable that person to apply for protection under the GDPR? Although there is consensus among legal scholars and commentators that the data used to create a deepfake should be treated as personal data, as it is assumed that in such a case the key criterion is identifiability, not data reality [Vallevik, Befring, Elvatun, et al. 2026, 44], there are some doubts as to whether simple similarity will actually be sufficient to attribute the deepfake to a specific person and enable them to seek protection of the personal data used by synthetic media [Öhman 2022, 3]. Such a situation may cause evidentiary difficulties, and the personal data protection process itself will be based not on the objective possibility of identification, but on the subjective perception of the recipient and on the context of the created deepfake.

Similar concerns arise when personal data is used to create a manipulated image. Specifically, this concerns the case where personal data is used by an AI model as source material to create a deepfake, but the generated material depicts entirely fictitious individuals [Romero Moreno 2024, 297]. In such a case, a completely different problem arises, related to the fact that the final product – the deepfake – will not enable identification of the person, even subjectively. However, the personal data of a specific person will, with high probability, be used in the creation process without their consent [Öhman 2022, 6]. The inability to demonstrate similarity with a real person will certainly make it difficult to prove that personal data was actually used in this particular case, which in turn may make it easier for the person responsible for generating the deepfake to avoid liability by invoking the complete synthetic nature of the generated audiovisual material.

The final example, which also raises considerable interpretational questions, concerns a situation where a deepfake uses the personal data of not just one person, but many at the same time. The artificial intelligence tools and models used to create manipulated videos, images, and sounds learn from the datasets shared with them. It is therefore possible that the resulting creation will be a deepfake that combines the characteristics

of multiple specific individuals. This makes it difficult to determine whether a given deepfake refers to a single person, multiple individuals, or perhaps no specific person. Who, in such circumstances, would have an effective right to request the erasure of their personal data?

These examples demonstrate that the emergence of deepfake technology fundamentally undermines the assumption underlying the protection of individuals embedded in the GDPR – that personal data always relates to a specific entity and can be easily identified. These problems arise, in particular, from the vague criterion of "identifiability," the volatile nature of digital data, and the use of multiple data sources from different individuals in the material generation process. This leads to a reduction in the effectiveness of the protective mechanisms that individuals have previously been able to benefit from.

In the context of reflections regarding the effectiveness of the right to be forgotten and its relationship to the new digital reality created by deepfakes, the issue of the almost instantaneous and unlimited multiplication of modified content generated by artificial intelligence cannot be ignored. This allows internet users to share deepfakes via multiple platforms simultaneously, as well as modify and publish them in modified versions. It should be noted that the digital environment is cross-border in nature [Erdos 2021, 2-3], which means the reach of deepfakes is limitless. From the perspective of personal data protection and the possibility of an individual requesting their erasure in the event of unauthorized use, doubts arise regarding the assumptions on which Article 17 of the GDPR is based. The effectiveness of the right to be forgotten relies on the premise that the controllers of personal data can be identified and that the data can be effectively erased from their collected resources. While this issue has already been discussed in the literature to some extent in relation to the difficulties that may arise when fulfilling a request to delete data in other cases [Politou, Alepis, and Patsakis 2018, 15-16], the deepfake technology elevates this problem to a completely different level.

Repeated copying, dissemination, and modification of the original version of deepfakes leads to difficulties in determining the entity to which the role of controller should be assigned [Gambín, Yazidi, Vasilakos, et al. 2024, 25]. The network of connections that forms between all participants in the digital environment also complicates the original controller's ability to fulfill its obligation under Article 17(2) of the GDPR. Furthermore, deletion of data by one controller does not provide assurance that the data are not actually located elsewhere. Finally, the ability to process and modify the original versions of deepfakes deprives the individual of the guarantee that deleting the original version of manipulated audiovisual material will prevent the creation of further ones. In reality, this leads to a loss of real

control over one's personal data and means that the guarantees contained in the GDPR provide personal data protection only fragmentarily, and in the remaining scope, they become illusory.

The problematic issues presented also have a significant impact on the realization of an individual's information autonomy. The inability to use an effective mechanism for removing information from the digital sphere that may violate an individual's privacy, dignity, or reputation means that an individual loses the ability to decide what information about them is collected and processed. This means that an individual loses the right to shape their own image.

CONCLUSIONS

The emergence and widespread use of deepfakes by internet users has revealed new challenges that individuals must face in the context of protecting their personal data and exercising the right to be forgotten. These problematic issues lead to the conclusion that the right to be forgotten, as currently implemented, is ineffective. Therefore, changes seem necessary, both in the perception of personal data as a right and in the mechanisms that streamline the implementation of the right to personal data protection.

The current model of personal data protection is based on three main assumptions: realism, statics, and control. First, it is recognized that personal data must refer to a specific, existing person [Purtova 2018, 42]. Therefore, they serve to describe a reality that, in the case of deepfakes, can be changed and modified. Hence, doubts arise as to whether the data generated in this process should still be considered personal data and subject to legal protection. Second, data is believed to be static in nature, meaning it is possible to extract and assign a specific set of information to a specific person [Hallinan and Gellert 2020, 273-274]. Deepfake technology, however, demonstrates that personal data are not finite sets of data but an ongoing process in which data can be generated, transformed, and combined. Third, the current model of personal data protection assumes that individuals have real control over the sharing of their personal data and its subsequent use by other entities [Kocharyan, Vardanyan, Hamuľák, et al. 2021, 98]. This control involves the use of mechanisms that allow individuals to access the data collected about them, the right to request rectification, and ultimately the right to request deletion. However, synthetic media have exposed this illusion, demonstrating that individuals cannot always effectively use the tools granted under Article 17(1) of the GDPR, especially when identifying the controller is difficult, or when the original deepfake and its subsequent versions are replicated [Rutkowska 2019, 210]. Current methods of personal data protection are based on an ineffective and outdated model,

which, in the context of generative AI, cannot rely solely on data deletion but should also address the relationships between personal data, the process of attributing them to an individual, and their subsequent dissemination.

Looking at deepfakes without considering contemporary realities leads to the erroneous assumption that manipulated content can be deleted. Once made available in the digital environment, these materials are disseminated on such a scale and by so many entities that removing them from the digital sphere and all other media is structurally impossible.

The legal commentary increasingly embraces the view that existing legal measures are insufficient and that individuals need to have greater control over their digitally processed personal data. Theories such as machine unlearning, deletion-as-confidence, and deletion-as-control are widely discussed [Cohen, Smith, Swanberg, et al. 2023, 9]. At the same time, the close connection between personal data and the way they are used and the process of creating an individual's identity is emphasized [Nowikowska 2025, 278-79]. Listening to these voices, it seems possible to introduce new solutions that could address the challenge posed by deepfake technology in the context of personal data protection and human identity, particularly digital one. It would certainly be naive to think that, in times of such intense development of artificial intelligence, it is possible to create a perfect model for personal data protection; however, it seems feasible to improve it in such a way that it becomes more effective and limits the potential for harm. Therefore, it is recommended that steps be taken to redefine the right to be forgotten, moving away from a narrow understanding of "data erasure" and toward a broader understanding of the individual's right to control their digital identity. This concept is based on the postulates of protecting not only the set of static personal data but also content generated within synthetic media, introducing preventive protection against violations, and expanding the scope of obligations of responsible entities.

Until now, the right to be forgotten has been treated rather as one of the tools for protecting an individual's digital identity, giving them control over their personal data [Maceratini 2024, 278]. However, in the current technological environment, it is worth considering a conceptual fusion and redefinition of the right to be forgotten in the context of protecting an individual's identity. The proposed change assumes a shift in the burden from personal data protection to the protection of broadly understood human identity, which also includes personal data [Michałkiewicz-Kądziela 2020, 17]. This legal guarantee would cover not only personal data with the status of information, but also other data used to create a digital identity, as well as the very process of using this data to present a person in the digital space. To ensure the effectiveness of this approach, the scope of current protection would also need to be expanded, extending the guarantee not only

to personal data in the classic sense, but also to all digital products that are based on personal data or that themselves constitute data, but are synthetic in nature (e.g., digital representations, synthetic voices, generated images, etc.). Such action, aimed at expressly stating that content generated by artificial intelligence is also subject to GDPR protection [Ganev and De Cristofaro 2026, 2], would certainly dispel the emerging doubts about whether a given deepfake violates our right to privacy and personal data [Lundgren 2025, 3]. Of course, it remains a matter of debate whether these would always have to be synthetic data that would potentially enable identification of a person, because then, theoretically, those whose personal data were used without their consent to create manipulated content would remain unprotected, but the deepfake itself, in its final form, does not enable personal identification. It should be noted, however, that the prevailing view among legal writers is that personal data protection covers every stage of deepfake creation, including the stage of training an artificial intelligence model on data sets [Romero Moreno 2024, 297].

The proposed redefinition of the right to be forgotten also aims to introduce a significant change regarding the timing of its protection. Currently, a request to delete personal data occurs after an actual situation of unauthorized data use. The protection model involves identifying the controller, identifying the personal data used, and simply requesting the deletion of this data from the virtual world. In the case of deepfakes, this process is complicated by the possibility of decentralization – it is difficult to locate the entity responsible, specific data, and deletion is often impossible due to the ease of multiplication. Waiting for a personal data breach weakens individual protection, as individuals can only react when the damage occurs *ex post* [Hacker, Engel, and Mauer 2023, 16] The proposed change in approach aims to develop preventive mechanisms that operate not at the moment of the event, but before the content is widely disseminated and during its circulation. Therefore, the aim is to introduce measures that will prevent and mitigate the risk of personal data breaches, not simply address their effects more or less effectively. The implementation of such measures should include expanding obligations imposed not only on controllers but also on the creators of deepfakes and online platforms (who are not always the controllers at this same time) [Becker, Thorogood, Bovenberg, et al. 2022, 208]. It would be desirable to introduce (in addition to labeling deepfakes, which is already included in the AI Act): a restriction on the ability of generative models to learn from personal data without the individual's consent; a proactive approach to detecting deepfakes and limiting their visibility; an obligation to secure deepfakes in a way that prevents re-uploading (stay-down obligation); and strengthening the effect of data deletion by introducing an obligation to inform other entities about the need to delete data, as well

as by introducing digital mechanisms that would assist in identifying copies of the original content. The aim of the new approach to the right to be forgotten is therefore not only to increase the scope of simple content deletion, but above all to give individuals control over the content disseminated about them.

The real problem that undermines the effectiveness of existing legal measures, but may also undermine the effectiveness of the proposed changes, is the lack of uniform, universal legal tools related to the operation of deepfakes in the digital sphere and the protection of personal data. The weakness of EU mechanisms is that they are effective only within the European Union, and deepfakes are cross-border in nature. Therefore, international cooperation is highly desirable, which will strengthen the effectiveness of global enforcement of protection of individual rights.

This does not change the fact that taking certain actions, even at the EU level, is essential, as maintaining the legal regulations regarding the right to be forgotten in their current form will lead to a continuous reduction in the effectiveness of tools for legal protection of individuals against digital threats due to rapid technological development. Therefore, the concepts proposed in this publication, which shift the focus from static data protection to a broader, conceptually based protection of human identity, as well as the proposal to take steps to provide individuals with real control over their digital representation by introducing ex ante mechanisms, seem to be a reasonable direction for change.

REFERENCES

Ahmed, Saifuddin, and Hui Wen Chua. 2023. "Perception and deception: Exploring individual responses to deepfakes across different modalities." *Heliyon* 9, no. 10:1-8.

Alanazi, Sami, and Semal Asif. 2024. "Exploring deepfake technology: creation, consequences and countermeasures." *Human-Intelligent Systems Integration* no. 6:49-60. https://doi.org/10.1007/s42454-024-00054-8

Becker, Regina, Adrian Thorogood, Jasper Bovenberg, et al.. "Applying GDPR roles and responsibilities to scientific data sharing." *International Data Privacy Law* 12, no. 3:207-19. https://doi.org/10.1093/idpl/ipac011

Clark, Simon, and Stephan Lewandowsky. 2026. "The continued influence of AI-generated deepfake videos despite transparency warnings." *Communications Psychology* 4, no.13: 1-12. https://doi.org/10.1038/s44271-025-00381-9

Cohen, Aloni, Adam Smith, Marika Swanberg, et al. 2023. "Control, Confidentiality, and the Right to be Forgotten." https://arxiv.org/abs/2210.07876 [accessed: 15.03.2026].

Cook, Lyndsay. 2015. "The right to be forgotten: a step in the right direction for cyberspace law and policy." *Journal of Law, Technology & the Internet* 6:121-32.

Erdos, David. 2021. "The 'right to be forgotten' beyond the EU: ananalysis of wider G20 regulatory action and potentialnext steps." *Journal of Media Law* 13, no. 1:1-35. https://doi.org/10.1080/17577632.2021.1884947

Gambín, Ángel F., Anis Yazidi, Athanasios Vasilakos, et al. 2024. "Deepfakes: current and future trends." *Artificial Intelligence Review* 57, no. 64:1-32. https://doi.org/10.1007/s10462-023-10679-x

Ganev, Georgi, and Emiliano De Cristofaro.2026. "Rethinking Anonymity Claims in Synthetic Data Generation: A Model-Centric Privacy Attack Perspective." https://arxiv.org/abs/2601.22434 [accessed: 20.03.2026].

Hacker, Philipp, Andreas Engel, and Marco Mauer. 2023. "Regulating ChatGPT and other Large Generative AI Models." https://arxiv.org/abs/2302.02337 [accessed: 20.03.2026].

Hallinan, Dara, and Raphaël Gellert. 2020. "The Concept of 'Information': An Invisible Problem in the GDPR." *Scripted* 17, no. 2:269-319. https://doi.org/10.2966/scrip.170220.269

Klimas, Anita M. 2024. "The 'right to be forgotten' and the right to freedom of expression and information-legal problems on the basis of the judgment of the Supreme Administrative Court of 9 February 2023." *Central European Academy Law Review* 2, no. 1:103-24.

Kocharyan, Hovsep, Lusine Vardanya, Ondrej Hamuľák, et al. 2021. "Critical Views on the Right to be Forgotten after the Entry into Force of the GDPR: is it Able to Effectively Ensure our Privacy?" *International and Comparative Law Review* 21, no. 2:96-115. https://doi.org/10.2478/iclr-2021-0015

Lundgren, Björn. 2025. "Can Deepfakes Violate an Individual's Moral Right to Privacy?" *Ethical Theory and Moral Practice* 29:125-39. https://doi.org/10.1007/s10677-025-10514-y

Maceratini, Adrianna. 2024. "Subjective Identity and the Right to be Forgotten: A Multifaceted Claim in the Legal System." *Bialystok Legal Studies* 29, no. 3:271-86. https://doi.org/10.15290/bsp.2024.29.03.15

Michałkiewicz-Kądziela, Ewa. 2020. *Prawo do tożsamości człowieka w prawie polskim i międzynarodowym*. C. H. Beck.

Nasiadka, Łukasz. 2023. "Prawo do bycia zapomnianym w perspektywie przetwarzania danych osobowych." *Studia Prawa Publicznego* 42, no. 2:77-94. https://doi.org/10.14746/spp.2023.2.42.3

Nowikowska, Monika. 2025. "Deepfakes in New Media – a Threat to Digital Identity." *Roczniki Kulturoznawcze* 16 no. 4:269-82. https://doi.org/10.18290/rkult25164.16

Öhman, Carl. 2022. "The identification game: deepfakes and the epistemic limits of identity." *Synthese* 200, no. 319:1-19. https://doi.org/10.1007/s11229-022-03798-5

Pawelec, Maria, and Mateusz Łabuz. 2025. "Deepfakes – Threats and Recommendations for Legal and Societal Action." CEE Digital Democracy Watch: Warsaw.

Politou, Eugenia, Efthimios Alepis, and Constatntinos Patsakis. 2018. "Forgetting personal data and revoking consent under the GDPR: Challenges and proposed solutions." *Journal of Cybersecurity* 0:1-20. https://doi.org/10.1093/cybsec/tyy001

Purtova, Nadezhda. 2018. "The law of everything. Broad concept of personal data and future of EU data protection law." *Law, Innovation and Technology* 10, no. 1:40-81. https://doi.org/10.1080/17579961.2018.1452176.

Romero Moreno, Felipe. 2024. "Generative AI and deepfakes: a human rights approach to tackling harmful content." *International Review of Law, Computers & Technology* 38, no. 3:297-326.

Ruschemeier, Hannah. 2025. "Generative AI and data protection." *Cambridge Forum on AI: Law and Governance* 1, no. 6:1-16. https://doi.org/10.1017/cfl.2024.2

Rutkowska, Patrycja. 2019. "Prawo do „bycia zapomnianym" w cyfrowym świecie." *Społeczeństwo i Polityka* 58, no. 1:199-213.

Sivarajah, Seyon, Lukas Heidemann, Alan Lawrence, et al. 2022. "Tierkreis: a Dataflow Framework for Hybrid Quantum-Classical Computing." IEEE/ACM Third International Workshop on Quantum Computing Software (QCS), Dallas, TX, USA:12-21. https://doi.org/10.1109/QCS56647.2022.00007

Vallevik, Vibeke Binz, Anne Kjersti C Befring, Severin Elvatun, et al. 2026. "Processing of synthetic data in AI development for healthcare and the definition of personal data in EU law." *International Journal of Law and Information Technology* 34:1-60. https://doi.org/10.1093/ijlit/eaag002

Van der Sloot, Bart, and Yvette Wagensveld. 2022. "Deepfakes: regulatory challenges for the synthetic society." *Computer Law and Security Review* 49:1-15.

Zhang, Dawen, Pamela Finckenberg-Broman, Thong Hoang, et al. 2025. "Right to be forgotten in the Era of large language models: implications, challenges, and solutions." *AI and Ethics* 5:2445-454. https://doi.org/10.1007/s43681-024-00573-9