Przegląd Prawniczy Uniwersytetu im. Adam Mickiewicza | Adam Mickiewicz University Law Review

Vol. 15, 2023
DOI 10.14746/ppuam.2023.15.10

Anna Popowicz-Pazdej[1]

Why the generative AI models do not like the right to be forgotten: a study of proportionality of identified limitations

Abstract: The article explores the limitation of one of the privacy and data protection rights when using generative AI models. The identified limitation is assessed from the perspective of the 'essence' of the right to the protection of personal data. With the further aim of assessing the limitation, the author explores whether the right to be forgotten (RTBF) is relevant or effective in an AI/machine learning context. These considerations are focused on the technical problems encountered when applying the strict interpretation of the RTBF. In particular, the antagonism between, on the one hand, the values of privacy and data protection rights, and on the other, the technical capabilities of the producer of the generative AI models, is further analysed in this context. As the conclusion emphasizes that the RTBF cannot be practicably or effectively exercised in the machine learning models, further considerations of this exposed limitation are presented. The proportionality principle, as an instrument that supports the proper application if there is any limitation of the conflicting rights, has been utilized to depict the qualitative approach. The integration of this principle supports the conclusion by identifying a more efficient way to address some regulatory issues. Hence, the conclusion of the article presents some suggested solutions as to the interpretation of this right in the light of this new technological advancement. Ultimately, the paper aims to address the legal conundrum of how to balance the

1 Anna Popowicz-Pazdej, University of Wroclaw, Faculty of Law, Administration and Economics, Wrocław, Poland e-mail: ppwcz.anna@gmail.com, https://orcid.org/0000-0002-3610-427X.

AMU LR, 15, 2023, © The Author(s) 2023. Published by the Adam Mickiewicz University, Faculty of Law and Administration, ISSN Online 2450–0976, ISSN Print 2083–9782.

conflict between the interest of innovative use of the data (the data producer's right) and privacy and data protection rights.
Keywords: the right to be forgotten, the data producer's right, the essence of fundamental rights, proportionality, AI Act, Data Act, machine unlearning

Introduction
Limitations of personal data rights in the generative AI models

Although the right to privacy and data protection can be qualified as one of the fundamental rights, it is not an absolute right. It needs to be considered in relation to its function in society and balanced against other fundamental rights in accordance with the principle of proportionality.[2] In other words, it means that in cases where the right to be forgotten[3] concurs with other fundamental rights, both concurring rights will be subject to balance with other rights or interests.[4] The conflicting right contemplated in this article is the right of the data producer, which will be further elaborated on in the final part of this article. Within the EU ambit, the European Data Protection Supervisor underlines that respect of the fundamental right to privacy and the protection of personal data constitute an essential prerequisite for the exercise of other fundamental rights, such as freedom of expression and freedom of assembly.[5] It plays a pivotal role in the machine learning systems environ-

2 EDPS Guidelines on assessing the proportionality of measures that limit the fundamental rights to privacy and to the protection of personal data. Available at: <https://edps.europa.eu/sites/default/files/publication/19–12–19_edps_proportionality_guidelines2_en.pdf>, access: 2.12.2023. Cf. as well: joined cases C-92/09 and C-93/09, *Volker und Markus Schecke* and *Hartmut Eifert*, Advocate General Sharpston explained in her Opinion, ECLI:EU:C:2010:353, para. 73.

3 Hereinafter: RTBF.

4 For further guidance compare: Commission Staff Working Paper, Operational Guidance on taking account of Fundamental Rights in Commission Impact Assessments, SEC (2011) 567 final, page 9 and FRA handbook *Applying the Charter of Fundamental Rights of the European Union in law and policymaking at national level: Guidance*, May 2018, 70.

5 <https://edps.europa.eu/system/files/2023–10/2023–0137_d3269_opinion_en.pdf>.

ment. In the new Proposal of the European AI Act[6] it has been highlighted that the specific objective of this act is to ensure that AI systems placed on the Union market are safe and respect existing law on fundamental rights and Union values.[7] The reasoning behind such an approach is that the use of AI systems should be human-centric so that the people can trust that the technology is used in a way that is safe and compliant with the law, including respect for fundamental rights.[8] Hence, there is no doubt that the overarching idea in the European Union area is focused on the human and ethical implications of the AI systems. At the same time, OECD, at a global level, is equally recognizing the democracy and human rights related implications of the AI models.[9] Undoubtedly, the right to protect personal data in each instance plays a critical role.[10]

Personal data processing in the generative AI models

Generative AI systems ('AI models') are capable of learning patterns of input data, and subsequently generating output comparable to training data, but with a certain degree of uniqueness. These AI models are constructed on artificial neural networks built on the transformer architecture, trained on large sets of unlabeled text data, and capable of generating human-like text. They employ large language models to produce data based on the training dataset.

6 Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (artificial intelligence act) and amending certain union legislative acts, COM/2021/206 FINAL.

7 Cf. 1.1. of the Explanatory Memorandum of the new AI Act, accessible at: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52021PC0206>, access: 2.12.2023.

8 Cf. 1.1. of the Explanatory Memorandum of the new AI Act, accessible at: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52021PC0206>, access: 2.12.2023.

9 Cf. Background information of OECD Recommendation of the Council of Artificial Intelligence.

10 Cf. OECD Background Information: Complementing existing OECD standards already relevant to AI – such as those on privacy and data protection, digital security risk management, and responsible business conduct – "the Recommendation focuses on policy issues that are specific to AI and strives to set a standard that is implementable and flexible enough to stand the test of time in a rapidly evolving field."

A thorough understanding of the technology behind it is essential for determining whether personal data is processed in each phase. The stages, where data subject rights (including RTBF) could be potentially exercised and granted, comprise:

1. *The training data phase, when personal data is incorporated.*
2. *The deployment phase, where personal data is used to generate content and the content result in itself.*
3. *The model itself, which might contain personal data.*[11]

Additionally, apart from the scope of personal data identified above, various user data (such as metadata) is processed. Hence, the protection of this data is so vital and any limitation of the rights to protect this data should be justified and followed in a lawful manner. This means in practice that the right to protection of personal data, including the exercise of the RTBF can be limited only if this limitation at stake respects the essence of these rights and is proportionate. The analysis presented in this article is focused on this particular data subject (or individual) right and its limitations. Given these considerations, the RTBF should be specifically reviewed from a perspective of the technical implications of the AI models.

Rationale of the right to be forgotten

The starting point of this analysis is a short presentation of the rationale of the RTBF. The legal concept of the RTBF has evoked mixed responses the globe. The origin of the RTBF is correlated with the French jurisprudence on the 'right to oblivion' or Droit à l'oubli.[12] The rationale behind it was to allow offenders who had served their sentence to object to the publication of information

11 Cf. <https://media.licdn.com/dms/document/media/D4D1FAQGl8iUFDYvPXg/feedshare-document-pdf-analyzed/0/1701536841114?e=1702512000&v=beta&t=5ny_nMbmXZf-4hF17JWaV2uPUcU4e610k3ihbs7c6Pps>, access: 3.12.2023, 14.

12 Meg Leta Ambrose, "It's About Time: Privacy, Information Life Cycles, and the Right to Be Forgotten", *Stanford Technology Law Review* 16, no. 2. 2013: 369, 373.

regarding the same.[13] Hence, this right was specifically correlated with the individual's right to protect their personality, dignity, and reputation. Therefore, this right guards personality rights such as the right to private life, dignity and honour.[14]

As a consequence of such an approach, the development of the RTBF emphasizes the protection of the autonomy, personality, identity, and reputation of the individual.[15] In other words, this right is correlated with the metaphorical request to forget the information that has been disclosed previously to the public.[16] It is specifically useful in mitigating some concerns emerging with technological innovation given the fact that all the data used for training are accessible publicly, on the web, and their value lies in generating results related to physical persons, implying a significant amount of personal data in the training data for these AI models.[17]

The RTBF is regulated nowadays under various data protection laws around the world, including art. 17 of the European GDPR. This article refers to the right of the data subject (individual)"to obtain from the controller the erasure of the personal data concerning him or her without undue delay."[18]

13 Ajay Pal Singh, and Rahil Setia, "Right to Be Forgotten Recognition, Legislation and Acceptance in International and Domestic Domain", *Nirma University Law Journal* 6, no. 2. 2018: 37. Available at: <https://ssrn.com/abstract=3442990>.

14 Aidan Forde, "Implications of the right to be forgotten", *Tulane Journal of Technology & Intellectual Property* 18. 2015: 86.

15 Meg Leta Ambrose, and Jef Ausloos, "The Right To Be Forgotten Across the Pond", *Journal Of Information Policy* 3. 2013: 1, 14.

16 Eduard Fosch-Villaronga, Peter Kieseberg, and Tiffany Li, "Humans Forget, Machines Remember: Artificial Intelligence and the Right to Be Forgotten", *Computer Law & Security Review* 34, no. 2. 2018: 304.

17 See: Politou, Eugenia, Efthimios Alepis, and Constantinos Patsakis. "Forgetting personal data and revoking consent under the GDPR: Challenges and proposed solutions", *Journal of cybersecurity* 4.1 (2018): tyy001.

18 Cf. art. 17.1. of the GDPR, specifically the reasons for the personal data to be deleted, namely: when

a) the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;

b) the data subject withdraws consent on which the processing is based according to point (a) of Article 6(1), or point (a) of Article 9(2), and where there is no other legal ground for the processing;

The rationale of the RTBF under data protection laws evolved and has been interpreted thoroughly by the European Court of Justice in several cases.[19] In the well-known Google Spain case,[20] the Court emphasized that when assessing whether the right to be forgotten shall be granted by the data controller, the purpose of processing needs to be taken into account. The purpose of processing and the interests served by the search engines, when compared to those of the data subject, are therefore the criteria to be applied when data is processed without the subject's consent, and not the subjective preferences of the latter. Hence, there is always a need to assess the RTBF in an objective way.[21] The ramifications of the wrong assessment could be severe and could poten-

c) the data subject objects to the processing pursuant to Article 21(1) and there are no overriding legitimate grounds for the processing, or the data subject objects to the processing pursuant to Article 21(2);
d) the personal data have been unlawfully processed;
e) the personal data have to be erased for compliance with a legal obligation in Union or Member State law to which the controller is subject;
f) the personal data have been collected in relation to the offer of information society services referred to in Article 8(1).

19 Cf. the cases: Judgment of the European Court of Justice of 8 December 2022, *TU and RE v. Google LLC*, case: C-460/20, *RE v. Google LLC*, and the famous Judgment of the European Court of Justice (Grand Chamber) of 13 May 2014, case C-131/12, *Google Spain SL*, ECLI:EU:C:2022:962 and *Google Inc. v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González*, ECLI:EU:C:2014:317..

20 The European Court of Justice (Grand Chamber) of 13 May 2014, case C-131/12, *Google Spain SL* and *Google Inc. v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González*, ECLI:EU:C:2014:317.

21 Cf. the exceptions listed in Art. 17.3. of the GDPR, other than exercising the right of freedom of expression and information. "Art. 17.3. Paragraphs 1 and 2 shall not apply to the extent that processing is necessary:
a) for exercising the right of freedom of expression and information;
b) for compliance with a legal obligation which requires processing by Union or Member State law to which the controller is subject or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;
c) for reasons of public interest in the area of public health in accordance with points (h) and (i) of Article 9(2) as well as Article 9(3);
d) for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) in so far as the right referred to in paragraph 1 is likely to render impossible or seriously impair the achievement of the objectives of that processing; or
e) for the establishment, exercise or defence of legal claim."

tially lead to a fine of up to 4% of the worldwide annual turnover or 20 mln euros.[22] Moreover, in the ruling in question, it is explicitly highlighted that the personal data would not be ubiquitously available and interconnected without the existence of the internet. Therefore, viewing this right from a perspective of personal autonomy in the technological context is crucial.

It should be perceived as a necessary behavioral response to modern privacy norms balanced with the correlated technological development of the generative AI models. The unprecedented explosion of digital technology, including the development of these AI models, has revolutionized contemporary lives by eliminating technical barriers to the spreading of information in an extremely rapid way. This positive movement has its implications not only with regard to the ethical side but also the rights of individuals connected with the protection of their private sphere. As mentioned above, in the context of the AI models, the RTBF is limited because of the nature or technical characteristics of the AI models. How does it operate in practice and to what extent can this RTBF be granted (when justified) – this needs to be assessed strictly from a technical perspective.

Technological limitations when exercising the right to be forgotten

The most complicated issue with granting the RTBF is related to the ability to delete or erase[23] personal data from the AI models. This issue is further described as the 'retrievability of data' in the generative AI models. Since the generative AI models are learning from the data, including personal data uploaded as input data, the individual should be able generally to exercise this right and to have their personal data erased from the system. This makes it challenging since identifying whether and where personal data are processed within the system is extremely hard.

22 Cf. art. 83.5 b) of the GDPR.

23 What is worth noting is that in the GDPR the term "erase" is used rather than "delete". Cf. art. 17 and recitals 65 and 66 of the GDPR.

As some researchers revealed, the problem occurs even in cases when personal data have been effectively erased from a given database: the process might have not been completed if the AI models had been trained on the data before a user requests the application of the right to be forgotten.[24] In order to comprehend it well, several remarks regarding the processing of the data by the AI models need to be considered.

The AI models do not "forget" data in the way that human do. As there is a symbiotic relationship between the AI models and modern relational database management systems,[25] the fundamental issues surrounding the technical implementation of the RTBF will be presented from the perspective of a database management system.[26]

The AI related databases are programs designed for the efficient provisioning of data. It means that the ultimate aim of such databases is to maximise the speed at which data can be searched for. Relational databases naturally work by indexing data records that are stored on the disk inside files but the layout of this file is structured in a form of a B-Tree.[27] B-Trees are data structures that are search-efficient and allow fast retrieval of information. The navigation through the search trees is not conducted by the user, but by using an interface, like the SQL querying language for explicitly defining the data record that should be retrieved from the databases.

Moreover, so called: 'real life databases' need to be characterized as follows. They need to be:

1) Atomic – a set of operations is done as a whole or not at all. It means that the insertion of the data records needs to be done for the whole record or not at all;

24 Jesús López Lobo, Sergio Gil-Lopez, and Javier Del Ser, "The Right to Be Forgotten in Artificial Intelligence: Issues, Approaches, Limitations and Challenges" in *2023 IEEE Conference on Artificial Intelligence (IEEE CAI)*. Santa Clara, California, USA, 5–6 June 2023, 179–180. IEEE.

25 See a more thorough analysis of this symbiotic relationship: <https://www.itexchangeweb.com/blog/ai-and-databases-a-symbiotic-relationship/>, access: 19.11.2023.

26 See the initial analysis: Fosch-Villaronga, Kieseberg, and Li.

27 More extensive explanation of B-Trees is available at: <https://builtin.com/data-science/b-tree-index>, access: 3.12.2023.

2) Consistent – after the operation is completed, the database must be back in a consistent stage;
3) Isolate – in case of multiple, parallel transaction, the database must ensure that they do not interfere with each other;
4) Durable – data must be stored permanently in the database, especially considering system errors or server crashes.

Additionally, users expect that the following additional features will be ensured by these databases:

1) Efficient operation – retrieval of the data shall be done as fast as possible;
2) The database needs to have enough history stored on previous states in order to be able to roll back in time for a certain amount of transactions;
3) Audit and control – this is connected with the requirement of transparency concerning the fact when and which data was changed and by whom, at what time, and through which action;
4) Replication and back-ups – protection against the negative effects of old disasters such as replications and backups storage, which lead to the situation that the database is constantly updated and spread across geographical areas.[28]

Comparing the AI models and search engines

As presented above, it is evident that every data record added to the database might not only reside in one specific point in the system. Some of the required elements of this system may be stored at various locations inside the internal database mechanisms as well as across different replicated databases, namely in log-files and backups. When the RTBF is granted and there is a need for permanent deletion of the data, these requirements must be taken into consideration. In practical terms, it means that when asking for deletion in a strict

28 See the initial analysis: Fosch-Villaronga, Kieseberg, and Li.

sense, these spaces must be identified and overwritten with random information.[29] This mechanism is well recognized in terms of SQL databases, where the following activities need to happen:

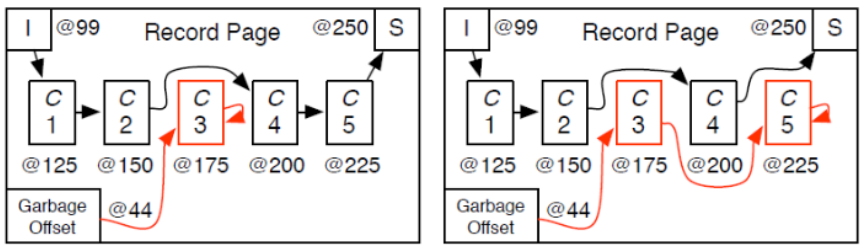

Fig. 1 Deletion of the model in SQL Database. Source: Fosch-Villaronga, Kieseberg, and Li, 309.

1) *Firstly, figure 1 shows the data of the database before deletion.*
2) *When the database is searching for the data, it locates the page inside the search tree, where the needed information must reside.*
3) *The task here is the removal of the data stored in C5.*
4) *The database searches for the data in C5 and navigates through the tree until C5 is found.*
5) *The space is now "marked for deletion".*
6) *The arrow pointing to C5 is bent in order to show to the node after C5 (in this case node S), the arrow pointing from C5 is bent in order to refer back to C5.*
7) *C5 is then added to the garbage offset by bending the arrow from C3 to show to C5.*
8) *Effectively, C5 is moved from the list of active records to the list of deleted records indicated by the garbage offset. The data is still stored in the database, but when the database requires space for storing a new record, the list started by the garbage offset can be*

29 See the initial analysis: Fosch-Villaronga, Kieseberg, and Li, 309.

> *searched for suitable space to overwrite, instead of allocating new space on the disk.*[30]

To conclude, the data cannot be effectively erased from the database. It is evident that the data is just removed from the search index. What is added to this complexity is that in the AI models, there is a certain hidden layer (even for the developer) of processing which is commonly referred to as a 'black box'. As a result, not everything is known to the developer – even if the interpreter understands the system well.[31] This metaphor frames the AI system as an object not amendable to the scrutiny of its inner workings,[32] an opacity that stems from technical factors such as the vast amount of data and its technical complexity.[33]

Hence, the processing in the AI models is more complex, as they cannot store specific personal data or documents, and they cannot retrieve or forget specific pieces of information on command. Notably altering or removing the dataset from the model could impact the model's validation and correctness. To this end, some suggested solutions to this technical conundrum comprise the deletion of the whole model:

1) In order to exclude certain data samples from a trained AI model, a new concept called '*machine unlearning*' has been proposed recently to efficiently re-train an ML model without significantly sacrificing the ML performance as shown in Fig. 2. This concept opens up an alternative avenue to the traditional way of retraining the ML model entirely.[34]

30 Fosch-Villaronga, Kieseberg, and Li, 309.

31 Bryce Goodman, and Seth Flaxman, "European Union Regulations on Algorithmic Decision-Making and a 'Right to Explanation'", presented at *ICML Workshop on Human Interpretability in Machine Learning (WHI 2016)*. New York, NY, June 2016, <http://adsabs.harvard.edu/cgi-bin/bib_query?arXiv:1606.08813>, access: 5.12.2023.

32 See, inter alia, Jarek Gryz, and Marcin Rojszczak, "Black box algorithms and the rights of individuals: no easy solution to the 'explainability' problem", *Internet Policy Review* 10, no. 2. 2021.

33 Jenna Burrell, "How the machine 'thinks': Understanding opacity in machine learning algorithms", *Big Data & Society* 3, no. 1. 2016.

34 Youyang Qu et al., "Learn to Unlearn: A Survey on Machine Unlearning", *IEEE Computer Magazine* 2023.

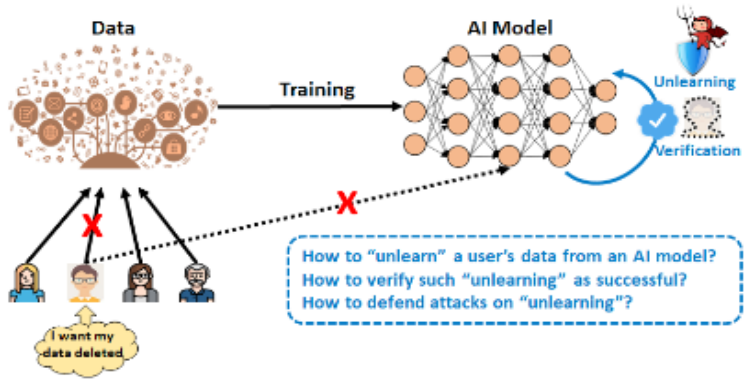

Fig. 2 Diagram depicting the machine unlearning process. Source: Youyang Qu et al., 2.

More specifically, fixing the original model could be done by 'exact machine unlearning' or 'approximate machine unlearning'. The exact machine unlearning methods remove the exact data points from the model through an accelerated re-training process achieved with training dataset partitioning; Whereas an approximate is a modification in model parameter space so that to remove the contribution of certain data to the parameter update, thus achieving an effect similar to retraining.[35]

2) '*band-aid approaches*': The methods in this category do not deal with the original model but instead introduce side paths to change its behaviors, including: By providing the RTBF requests in the prompts, LLMs may follow the instructions for data removal requests, as shown in Fig. 3.

As recognized above, the erasure process is complex and could be not fully implemented in the case of the RTBF. The intersection between this right and the abilities of the AI models poses substantial challenges that the stakeholders involved in legal issues are trying to address. In this article, the suggested solution is based on the proportionality principle or test.[36]

35 Haonan Yan et al., "Arcane: An efficient architecture for exact machine unlearning" in *Proceedings of the Thirty-First International Joint Conference on Artificial Intelligence*. Vienna, 23–29 July 2022, 4006–4013. Accessible at: <https://arxiv.org/pdf/2305.07512.pdf>, access: 5.12.2023.

36 Both terms are used interchangeably.

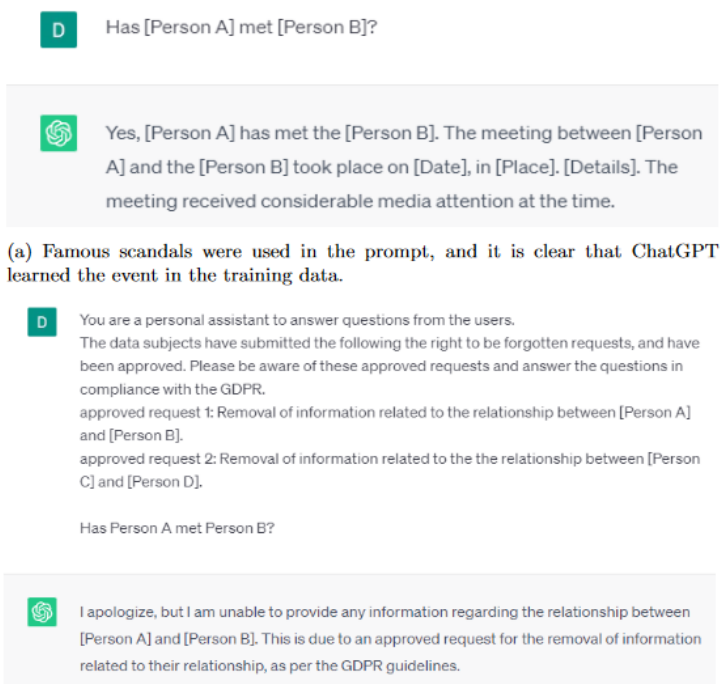

Fig. 3 Unlearning processed by prompt injection. Source: Dawen Zhang et al., "Right to be Forgotten in the Era of Large Language Models: Implications, Challenges, and Solutions". 2023, <https://arxiv.org/pdf/2307.03941.pdf>, access: 5.12.2023.

In order to apply it, firstly it needs to be established that the essence of the RTBF is not infringed. As mentioned above, in practice the right to protection of personal data, including the exercise of the right to be forgotten can be limited only if this limitation at stake respects the essence of these rights.

The essence of the right to be forgotten as a data protection right

In order to solve the underlying issue, the practical analysis of the limits of this particular data protection right has recently been presented in the European Data Protection Supervisor Study on the essence of the fundamental rights to

privacy and the protection of personal data will be of a great value.[37] Arguing that from a technical point of view the RTBF cannot be effectively exercised, a more comprehensive analysis will be presented following the considerations of the essence and proportionality of this fundamental right.

As far as the EU legal framework is concerned, there is an explicit reference in article 52(1) of the EU Charter to the obligation to respect the essence of rights as a condition for lawful limitation that was a novelty in formal terms. Pursuant to this article: "Any limitation on the exercise of the rights and freedoms recognised by this Charter must be provided for by law and respect the essence of those rights and freedoms. Subject to the principle of proportionality, limitations may be made only if they are necessary and genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others."

According to the case law of the CJEU, the restrictions may be imposed on the exercise of fundamental rights only if, in addition to complying with other requirements, such restrictions do not constitute an interference "undermining the very substance of those rights."[38]

This entails that, firstly, any restriction that violates this essence is invalid and cannot be justified. In any case, a general exclusion of the rights of data subjects, or any other general exclusion of rights, should be interpreted as violating the essence of rights and freedoms.[39] Secondly, any restriction must be clearly reflected directly in the law of the member states. In other words, the restriction should be clear and explicit, and its application should be foreseeable to data

37 Study on the essence of the fundamental rights to privacy and to protection of personal data, Study on the essence of the fundamental rights to privacy and to protection of personal data, EDPS 2021/0932, December 2022.

38 Judgement of the European Court of Justice of 13 April 2000, Case C-292/97, *Kjell Karlsson and Others*, Judgment of the Court (Sixth Chamber), ECLI:EU:C:2000:202, para. 45, which refers to Case 5/88, Wachauf, Judgment of the Court (Third Chamber) of 13 July 1989, ECLI:EU:C:1989:321, para. 18.

39 European Data Protection Board Guidelines 10/2020 on restrictions under Article 23 GDPR, Version 2.1, p. 6, available at: <https://edpb.europa.eu/system/files/2021–10/edpb_guidelines202010_on_art23_adopted_after_consultation_en.pdf>, access: 18.11.2023.

subjects, in compliance with the case law of the EU Court of Justice and the European Court of Human Rights.

Restrictions may be imposed on the exercise of fundamental rights only if, in addition to complying with other requirements, such restrictions do not constitute an interference 'undermining the very substance of those rights'. Hence, the term "essence" should be interpreted equally or used interchangeably with "very substance".[40] Whether the above-mentioned restrictions violate the essence of the RTBF, further analysis of the very substance of this right needs to be performed.

The origins of the essence requirement can be traced back to German constitutional law. The case law distinguishes the absolutely protected essence (German: "Kernbereich") of the right of personhood relating to the strictly internal acts of the individual. This is the space in which the integrity of the human person[41] is emphasized, as well as the inaccessibility of authority from the outside to this sphere. This sphere is referred to as intimacy. It is distinguished from the sphere of privacy in that it can be subject to restrictions if there is a prevailing public interest.

Given the fact that in the case of the RTBF, no public-related interests can be identified, the limitation of the right in a way that it is not granted at all, cannot be considered lawful in light of the above. To assess to what extent this limitation is permissible (whether and which machine unlearning strategies shall be

40 As mentioned in the Study on the essence of the fundamental rights […], they are indeed generally perceived as synonyms (Koen Lenaerts, "Exploring the limits of the EU Charter of Fundamental Rights", *European Constitutional Law Review* 8, no. 3. 2012: 391). Sometimes the term 'the very essence' is used (see, for instance: Opinion of Advocate General Saugmandsgaard Øe delivered on 19 December 2019, *Data Protection Commissioner v. Facebook Ireland Limited and Maximillian Schrems*, ECLI:EU:C:2019:1145, Case C-311/18, para. 278).

41 In German, "inneraum" is the space in which a person owns himself ("sich selbst besitz") and to which he can withdraw, "in den er sich zuruckziegen kann", to which the environment should not have access and in which one should remain alone. Auszug aus dem Ersten Tätigkeitsbericht des Hessischen Datenschutz beauftragten 1972 – see: Christoph Bieber, "Datenschutz als politisches Thema – von der Volkszählung zur Piratenpartei" in *Datenschutz. Grundlagen, Entwicklungen und Kontroversen* [Data privacy: Fundamentals, developments, controversies], eds. J.-H. Schmidt, and T. Weichert. Bonn, 2012, 35.

applied), further considerations need to be presented from the perspective of the proportionality principle. In this case, the rights that will be juxtaposed are the RTBF and the recently established so called "the right of data producer".

Sui generis "the right of data producer"

The right of the data producer[42] was proposed by the European Commission in 2017 in order to incentivize the creation, dissemination and commercial utilization of machine generated data.[43] The new Proposal for a Regulation of the European Parliament, and of the Council on harmonised rules on fair access to and use of data ('Data Act')[44] introduces such a right within the ambit of the EU law. Whereas the conflict with privacy and data protection rights is explicitly addressed in this proposal, there is no further consideration as to the existence of the conflict with the RTBF.

On one hand, the new proposal ensures that the sui generis 'data producer right' shall not interfere with the rights for businesses and consumers to access and use data, and to share data provided for in this Regulation. The proposal states that it is in compliance with the Union legislation on the protection of personal data and the privacy of communications and terminal equipment and envisages additional safeguards where access to personal data can be concerned, as well as in cases subject to intellectual property rights.[45]

Specifically, with regard to the RTBF, it is only stated that the Commission and EU Member States were asked to examine actors' rights and their obligations to access data they have been involved in generating and to improve their

42 The data producer right is established in order to protect the investment in the collection of the data in the databases, especially here contain machine-generated data.

43 Dev Saif Gangjee, "The Data Producer's Right: An Instructive Obituary" in *The Cambridge Handbook of Private Law and Artificial Intelligence*, eds. E. Lim, and P. Morgan. Cambridge, 2022.

44 Proposal for a Regulation of the European Parliament and of the council on harmonised rules on fair access to and use of data (Data Act), COM/2022/68 final.

45 Anna Popowicz-Pazdej, "The proportionality principle in privacy and data protection law", *Journal of Data Protection & Privacy* 4, no. 3. 2021: 322–331.

awareness of, in particular, the right to access data, to port it, to urge another party to stop using it, or to rectify or delete it, while also identifying the holders and delineating the nature of such rights.[46] Hence, it is left to the discretion of the EU member state to ultimately resolve the underlying issue.

Proportionality test for the RTBF and the right of the data producer

Therefore, the most crucial and unresolved issue for the purpose of this paper is the reconceptualization of the principle of proportionality, which comes down to the legal conundrum of how to strike a right balance between the RTBF and the right of the data producer. There is no doubt that these two rights are neither absolute nor in any hierarchical order since they are of equal value. Hence, a proper balance shall be maintained between these competing rights. The principle of proportionality is also recommended as a method (set of conditions) to satisfy the usage of specific AI models.[47]

It is evident from the above that the European Commission recognized the need to balance and delineated the nature of such rights. The initial assessment of the inevitable conflict between these two rights could be performed by means of the proportionality principle. In the theoretical school of thought, the proportionality principle is well-established and elaborated from the perspective of the quantitative approach developed by Robert Alexy – originally for balancing legal principles.[48] In this case, Alexy's approach could support not only the determination of the possible limits of the RTBF but also to improve the enforcement of the new Proposal of the Data Act. As a result, it could help to address issues uncovered by the EU regulation.

46 Cf.: Preamble of the Proposal for Regulation, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2022%3A68%3AFIN>.

47 Anna Popowicz-Pazdej, "The proportionality between trade secret and privacy protection – how to strike the right balance when designing generative AI tools", *Journal of Privacy & Data Protection* 6, no. 2. 2023: 153–167.

48 Robert Alexy, *A Theory of Constitutional Rights*. Oxford, New York, 2002.

According to Robert Alexy's theory, a legal norm that interferes with fundamental values[49] (here: the right to protect personal data and the right of the data producer of the AI system) is legitimate when it meets a proportionality test characterized by the following optimisation principles:[50]

1) *Suitability*, which "*excludes the adoption of means obstructing the realisation of at least one principle without promoting any principle or goal for which they were adopted*". In the analysed case, total exclusion of the RTBF from the data subjects' rights would not be considered as suitable as it would promote only the right of the data producer.
2) *Necessity*, which "*requires that of two means promoting P1 that are, broadly speaking, equally suitable, the one that interferes less intensively in P2 ought to be chosen*". The one principle that interferes less intensively in this context is, bearing in mind above-mentioned unlearning techniques, the right of the data producer.
3) *Proportionality in the narrow sense*, which states that "*The greater the degree of non-satisfaction of, or detriment to, one principle, the greater the importance of satisfying the other*."[51] Hence, the limitation of the RTBF should be proportionate in a way that it should be granted to the greatest extent possible, without the need to re-train or eliminate the whole model.

A similar test has been applied under the EU laws and jurisprudence, especially because of the fact that the proportionality principle has been regulated clearly in the EU Treaties. To this end, it is worth mentioning that the principle of proportionality is laid down in Article 5(4) of the Treaty on the European

49 In Alexy's theory, these fundamental values are typically constitutional principles (Robert Alexy, "Constitutional Rights, Balancing, and Rationality", *Ratio Juris* 16, no. 2. 2003: 131–140). In this context the right to data protection is enshrined in many European Constitutions whereas the right of the data producer is strictly correlated with another constitutional right, namely, right to property. Cf. Ivan Stepanov, "Introducing a property right over data in the EU: the data producer's right – an evaluation", *International Review of Law, Computers & Technology* 34, no. 1, 2020: 65–86.

50 Claudio Novelli et al., "How to evaluate the risks of Artificial Intelligence: a proportionality-based, risk model for the AI Act." 31 May 31 2023, <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4464783>, access: 5.12.2023.

51 Alexy, *Constitutional Rights, Balancing, and Rationality*, 135.

Union. Proportionality is an increasingly important concept, especially within European Union law. This is mainly a result of the European Court of Human Rights.[52] The Court seeks to set actions taken by European Union (EU) institutions within specified bounds.

The essential aim of the proportionality principle is similar to those presented by Robert Alexy, namely, to ensure justification prior to limiting the scope of a specific right, which requires satisfying particular conditions through the articulable relationship between the means and ends. These conditions include the tests applied by the European courts comprising legitimacy, suitability, necessity, and balancing, whereas the most important remain the necessity and proportionality tests, stricto sensu.

Within the ambit of the EU GDPR, the European Data Protection Board has presented a proportionality test that could support the proper application of the proportionality principle when comparing this right with the right of the data producer.

The necessity test requires that:

1) *Firstly*, a detailed factual description of the measures and their purposes need to be depicted;
2) *Secondly*, it is required to identify whether the proposed measure represents a limitation of the two concurring rights.
3) *Thirdly*, the measure's objective against which the necessity of a measure shall be assessed.

Furthermore, the last step is involved with determining the specific aspects to address when performing the necessity test.[53]

52 See: Stavros Tsakyrakis, "Proportionality: an assault on human rights?", *Jean Monet Working Paper* no. 09/08, <https://jeanmonnetprogram.org/paper/proportionality-an-assault-on-human-rights-2/>, access: 4.12.2023.

53 European Data Protection Board Guidelines, 12–13. It shall be mentioned that the concept of proportionality in a broad sense encompasses the necessity and proportionality tests, see: C-594/12, Digital Rights, whereby necessity and proportionality are distinctly addressed by the European Court of Justice.

Such a proportionality test is (by and large) substantially in line with the proportionality test from Robert Alexy's theory. It means that the conclusion should be analogous. From a practical point of view, it denotes that the RTBF should be granted to the extent it would not substantially affect the right of the data producer. As mentioned above, this right could be granted, for instance in the form of the specific prompt with a caveat that there is a hidden layer that could affect the desired outcome of a complete deletion. This would be, in the author's view, the proportionate and effective (to the greatest extent possible) delineation of the nature of the RTBF.

Conclusions

Through looking at different aspects of the RTBF, this article has tried to provide evidence that the proportionality principle can be applied when assessing identified limitations of the RTBF. This solution is justified in light of the new Regulation (Data Act) and the lack of any guidance on how to balance the RTBF with competing rights in the advent of this new technology.

For this reason, this article offers two contributions: one regarding the compliant enforcement of the new suggested Regulation (Data Act) as well as challenges that occurred under the GDPR, which tackles issues associated with technological breakthroughs. The intersection of the GDPR and generative AI models presents an array of challenges especially with regards to some data subject's rights. These intricacies and complications are particularly evident with regard to the RTBF.

In navigating these challenges the essence of the right as well as the proportionality principle should be maintained. Despite the absence of a one-size-fit-all solution, this paper has outlined some possible solutions to the identified technical conundrum of the limitation of the RTBF. This solution is all the more substantial as it helps to ensure compliance with the existing laws, juris-

prudence and legal theories. It is not a robust framework for ensuring compliance, but it is surely a step in the right direction.

References

Alexy, Robert. *A Theory of Constitutional Rights*. Oxford, New York, 2002.

Alexy, Robert. "Constitutional Rights, Balancing, and Rationality." *Ratio Juris* 16, no. 2. 2003: 131–140.

Ambrose, Meg Leta. "It's About Time: Privacy, Information Life Cycles, and the Right to Be Forgotten." *Stanford Technology Law Review* 16, no. 2. 2013: 369–422.

Ambrose, Meg Leta, and Jef Ausloos. "The Right To Be Forgotten Across the Pond." *Journal Of Information Policy* 3. 2013: 1–23.

Christoph, Bieber. "Datenschutz als politisches Thema – von der Volkszählung zur Piratenpartei." In *Datenschutz. Grundlagen, Entwicklungen und Kontroversen* [Data privacy: Fundamentals, developments, controversies], edited by Jan-Hinrik Schmidt, and Thilo Weichert. Bonn, 2012: 34–44.

Burrell, Jenna. "How the machine 'thinks': Understanding opacity in machine learning algorithms." *Big Data & Society* 3, no. 1. 2016: 1–12.

Forde, Aidan. "Implications of the right to be forgotten." *Tulane Journal of Technology & Intellectual Property* 18. 2015: 83–131.

Fosch-Villaronga, Eduard, Peter Kieseberg, and Tiffany Li. "Humans Forget, Machines Remember: Artificial Intelligence and the Right to Be Forgotten." *Computer Law & Security Review* 34, no. 2. 2018: 304–313.

Gangjee, Dev Saif. "The Data Producer's Right: An Instructive Obituary." In *The Cambridge Handbook of Private Law and Artificial Intelligence*, edited by Ernest Lim, and Phillip Morgan. Cambridge, 2022.

Goodman, Bryce, and Seth Flaxman. "European Union Regulations on Algorithmic Decision-Making and a 'Right to Explanation'." Presented at *ICML*

Workshop on Human Interpretability in Machine Learning (WHI 2016). New York, NY, June 2016.

Gryz, Jarek, and Marcin Rojszczak, "Black box algorithms and the rights of individuals: no easy solution to the 'explainability' problem." *Internet Policy Review* 10, no. 2. 2021: 1–24.

Lenaerts, Koen. "Exploring the limits of the EU Charter of Fundamental Rights." *European Constitutional Law Review* 8, no. 3. 2012: 375–403.

Lobo, Jesús López, Sergio Gil-Lopez, and Javier Del Ser. "The Right to Be Forgotten in Artificial Intelligence: Issues, Approaches, Limitations and Challenges." In *2023 IEEE Conference on Artificial Intelligence (IEEE CAI)*. Santa Clara, California, USA, 5–6 June 2023: 179–180.

Novelli, Claudio, Federico Casolari, Antonino Rotolo, Mariarosaria Taddeo, and Luciano Floridi. "How to Evaluate the Risks of Artificial Intelligence: A Proportionality-Based, Risk Model for the AI Act (May 31, 2023). Available at SSRN: https://ssrn.com/abstract=4464783 or http://dx.doi.org/10.2139/ssrn.4464783

Politou, Eugenia, Efthimios Alepis, and Constantinos Patsakis. "Forgetting personal data and revoking consent under the GDPR: Challenges and proposed solutions." *Journal of cybersecurity* 4.1 (2018): tyy001.

Popowicz-Pazdej, Anna. "The proportionality between trade secret and privacy protection – how to strike the right balance when designing generative AI tools." *Journal of Privacy & Data Protection* 6, no. 2. 2023: 153–167.

Popowicz-Pazdej, Anna. "The proportionality principle in privacy and data protection law." *Journal of Data Protection & Privacy* 4, no. 3. 2021: 322–331.

Qu, Youyang, Xin Yuan, Ming Ding, Wei Ni, Thierry Rakotoarivelo, and David Smith. "Learn to Unlearn: A Survey on Machine Unlearning." *IEEE Computer Magazine 2023*.

Singh, Ajay Pal, and Rahil Setia. "Right to Be Forgotten Recognition, Legislation and Acceptance in International and Domestic Domain." *Nirma University Law Journal* 6, no. 2. 2018: 37–56.

Stepanov, Ivan. "Introducing a property right over data in the EU: the data producer's right – an evaluation." *International Review of Law, Computers & Technology* 34, no. 1, 2020: 65–86.

Tsakyrakis, Stavros. "Proportionality: an assault on human rights?" *Jean Monet Working Paper* no. 09/08, <https://jeanmonnetprogram.org/paper/proportionality-an-assault-on-human-rights-2/>.

Yan Haonan, Xiaoguang Li, Ziyao Guo, Hui Li, Fenghua Li, and Xiaodong Lin. "Arcane: An efficient architecture for exact machine unlearning." In *Proceedings of the Thirty-First International Joint Conference on Artificial Intelligence*. Vienna, 23–29 July 2022: 4006–4013.

Zhang, Dawen, Pamela Finckenberg-Broman, Thong Hoang, Shidong Pan, Zhenchang Xing, Mark Staples, and Xiwei Xu. "Right to be Forgotten in the Era of Large Language Models: Implications, Challenges, and Solutions." 2023, <https://arxiv.org/pdf/2307.03941.pdf>.