Catholic University Journal of Law and Technology

Volume 31
Issue 1 *Fall 2022*

Article 5

2022

The Application of the Right to be Forgotten in the Machine Learning Context: From the Perspective of European Laws

Zeyu Zhao

Follow this and additional works at: https://scholarship.law.edu/jlt

 Part of the Business Intelligence Commons, Business Law, Public Responsibility, and Ethics Commons, Cataloging and Metadata Commons, Collection Development and Management Commons, Commercial Law Commons, Communications Law Commons, Communication Technology and New Media Commons, Comparative and Foreign Law Commons, Computer Law Commons, Conflict of Laws Commons, Consumer Protection Law Commons, Economic Policy Commons, European Law Commons, Human Rights Law Commons, Intellectual Property Law Commons, International and Intercultural Communication Commons, International Law Commons, Internet Law Commons, Law and Society Commons, Legislation Commons, Mass Communication Commons, Privacy Law Commons, Public Affairs Commons, Science and Technology Law Commons, Science and Technology Policy Commons, Science and Technology Studies Commons, Social Policy Commons, and the Technology and Innovation Commons

Recommended Citation

Zeyu Zhao, *The Application of the Right to be Forgotten in the Machine Learning Context: From the Perspective of European Laws*, 31 Cath. U. J. L. & Tech 73 (2022).
Available at: https://scholarship.law.edu/jlt/vol31/iss1/5

This Article is brought to you for free and open access by Catholic Law Scholarship Repository. It has been accepted for inclusion in Catholic University Journal of Law and Technology by an authorized editor of Catholic Law Scholarship Repository. For more information, please contact edinger@law.edu.

THE APPLICATION OF THE RIGHT TO BE FORGOTTEN IN THE MACHINE LEARNING CONTEXT: FROM THE PERSPECTIVE OF EUROPEAN LAWS

Zeyu Zhao[*]

[*] PhD Candidate, Renmin University of China; I highly appreciate the valuable instruction and feedback given by Dr. Asma Vranaki as well as the commendable work of the editors of *The Journal of Law and Technology*.

"AI enters the house through the Cloud."[1] Artificial Intelligence (AI) has nearly reached each corner of the daily routine and become one of the driving components of society.[2] As a representative technology in the AI high-tech arsenal, machine learning ("ML") has also consciously or subliminally pervaded the society.[3] This is echoed by Tony Tether, the former director of the United States Defense Advanced Research Projects Agency (DARPA), noting that ML is considered the future of the Internet.[4] While this technology is challenging and changing our ordinary lifestyles through its supposedly better intelligence and vision, it inevitably has drawbacks for society.[5] For instance, the Google DeepMind ML system may positively solve significant concerns such as global warming and energy waste.[6] Yet, it might lead to negative consequences for human ethics and rights.[7]

While it is uncertain if the right to be forgotten (RTBF) can be recognized as a fundamental human right due to the merits of privacy, self-determination, and

---

1 *See* Ronald Leenes & Silvia De Conca, *Artificial Intelligence and Privacy - AI Enters the House Through the Cloud*, *in* RESEARCH. HANDBOOK ON THE LAW OF A.I. 280, 280 (Woodrow Barfield & Ugo Pagallo eds., 2018).

2 *See* Select Committee on Artificial Intelligence, AI in the UK: Ready, Willing and Able?, 2017-19, HL 100, ¶ 3 (UK).

3 *See* Science and Technology Committee, Robotics and Artificial Intelligence, 2016–17, HC 145, ¶ 5 (UK).

4 *See* Woodrow Barfield, *Towards a Law of Artificial Intelligence*, *in* RESEARCH. HANDBOOK ON THE LAW OF A.I. 2, 3 (Woodrow Barfield & Ugo Pagallo eds., 2018).

5 *See* Ashley Deeks et al., *Machine Learning, Artificial Intelligence, and the Use of Force by States*, 10 J. NAT'L SEC. L. & POL'Y 1, 1–2 (2019); *see generally* Ekaterina Semenova et al., *Fairness Meets Machine Learning: Searching for a Better Balance* (Nat'l Rsch. U. Higher Sch. of Econ., Working Paper No. 93, 2019).

6 *See* Michael Guihot et al., *Nudging Robots: Innovative Solutions to Regulate Artificial Intelligence*, 20 VAND. J. ENT. & TECH. L. 385, 388 (2017).

7 *Id.* at 404.

reputation that it presents,[8] it is at least under the framework of data protection rights. Personal data rights have long been recognized as a kind of fundamental human right in Europe and most states in the world.[9] They can also be indirectly intertwined with the right to privacy as another cluster of human rights encoded in the European Union's (EU) Charter of Fundamental Rights, because the protection of personal data is also viewed as a form of privacy right including "bodily integrity, access to information and public documents, secrecy of correspondence and communication, protection of the domicile."[10] Although it differs from the right to data protection in terms of the scope of application and the justification standards for processing, the connection between RTBF and the right to privacy could be established if the information to be erased involves "private life", and the "forgetting of information" meets the conditions of "interference with privacy" according to a broader assessment of the democratic value.[11] In dual ways, RTBF ensures the preservation of human rights. Since ML may adversely affect human rights, RTBF should be altered and reformed in line with machinery features for more effective protection. Nevertheless, it seems that the current legal framework for RTBF in Europe, including Articles 17, 18, and 19 of the General Data Protection Regulation (GDPR), is unable to achieve this goal in the age of ML.[12] This means that personal data containing information related to an identified or identifiable natural person (data subject) is unlikely to be effectively "forgotten" by the operations of data controllers and processors who use ML agents to process personal data under data subjects' requests.[13] This is partly because there is inconsistency in legal, technical, and

---

8 *See* Oskar J. Gstrein, *Right to Be Forgotten: European Data Imperialism, National Privilege, or Universal Human Right?*, 13 REV. EUR. ADMIN. L. 125, 126 (2020); Andrew Neville, *Is It a Human Right to be Forgotten? Conceptualizing the World View*, 15 SANTA CLARA J. INT'L L. 157, 170–71 (2017); *see also* Simon Wechsler, *The Right to Remember: The European Convention on Human Rights and the Right to Be Forgotten*, COLUM. J.L. & SOC. PROBS. 135, 145–46 (2015); David Lindsay, *The 'Right to be Forgotten' in European Data Protection Law, in* EMERGING CHALLENGES IN PRIVACY LAW: COMPARATIVE PERSPECTIVE, 290, 290–91 (Normann Witzleb et al. eds., 2014).

9 Charter of Fundamental Rights of the European Union, art. 8, 2012 O.J. (C 326) 397; *see* International Conference of Data Protection & Privacy Commissioners, *International Resolution on Privacy as a Fundamental Human Right and Precondition for Exercising Other Fundamental Rights* (Oct. 21–24, 2019).

10 Raphaël Gellert & Serge Gutwirth, *The Legal Construction of Privacy and Data Protection*, 29 COMPUT. L. & SEC. REV. 522, 524 (2013); *see also* Charter of Fundamental Rights of the European Union, art. 7, 2012 O.J. (C 326) 397; *see generally* European Convention on Human Rights, art. 8, Aug. 1, 2021, 15 C.E.T.S. 213.

11 *See* Juliane Kokott & Christoph Sobotta, *The Distinction Between Privacy and Data Protection in the Jurisprudence of the CJEU and the ECtHR*, 3 INT'L DATA PRIV. L. 222, 226–27 (2013).

12 *See* Eduard Fosch Villaronga et al., *Humans Forget, Machines Remember: Artificial Intelligence and the Right to be Forgotten*, 34 COMPUT. L. & SEC. REV. 304, 304–05 (2018).

13 Regulation 2016/679 of the European Parliament and of the Council of 27 of April

conceptual spheres among RTBF rules in Europe, particularly GDPR and the relevant case law and the ML systems.

This article will probe into the essence of ML and the evolution of RTBF in European laws and argue that there are loopholes and defects when applying the current RTBF rules in the ML context. This article will also seek potential solutions to these applicability issues with the help of cyberspace regulation theories. It will point out the critical components of the ML operation including algorithms, big data, and neuron networks and analyze their working mechanisms in various categories of ML systems. Then it will describe the origin of RTBF, the related provisions in GDPR, and the case law about this right, the latter two of which constitute a sound legal framework. Next this paper will explore the deficiencies in coherently applying this right in European laws under the ML background. Specifically, it will argue that the application of RTBF could face challenges from the perspectives of structure, instructiveness, and criteria settings of the law and the practical landscape of ML progress. These issues can be concluded with two categories: a lack of guidance within the EU laws and the practical barriers to enforcing the laws. The practical obstacles include the finiteness of forgetting, unclear forgetting standards and intricate value balance. Finally, it will visit cyberspace regulation theories such as the Network Communitarianism and ANT-Foucauldian Power Lens and focus on the guardianship or stewardship responsibilities for online intermediaries, which ask them to make technical, legal, and other solutions for the RTBF.[14]

To formulate the above viewpoints and conclusions, this article will adopt the doctrinal methodology to review the profound history of RTBF in European traditions, dissect the institutionalized *modus operandi* for applying this right enshrined in GDPR and the relevant case law, and figure out how to implement its rules and principles against the ML backdrop in an integrative way of research. Accordingly, this article will mainly research into the primary legal materials including Articles 17, 18 and 19 of the GDPR, notable cases like *Google Spain*,[15] *NT1, NT2*[16] and *Google v. CNIL*[17] as well as some practical

---

2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), art. 4, 2016 O.J. (L 119/1) 1, 24 [hereinafter GDPR].

14 *See generally* CHRIS REED & ANDREW MURRAY, RETHINKING THE JURISPRUDENCE OF CYBERSPACE (2018); Asma A. Vranaki, *Regulating Social Networking Sites: Facebook, Online Behavioral Advertising, Data Protection Laws and Power*, 43 RUTGERS COMPUT. & TECH. L. J. 168, 172, 176–77 (2017).

15 *See generally* Case C-131/12, Google Spain SL v. Agencia Española de Protección de Datos, ECLI:EU:C:2014:317 (May 13, 2014).

16 *See generally* NT1 & NT2 v. Google Inc., [2018] EWHC (QB) 799 (Eng.).

17 *See generally* Case C-507/17, Google Inc. v. Comm'n Nationale de l'Informatique et des Libertés, ECLI:EU:C:2019:772 (Sept. 24, 2019).

instructions at the member state level.

I. MACHINE LEARNING AND THE RIGHT TO BE FORGOTTEN

A. The Background of Machine Learning

ML aims to learn knowledge and improve the computing skills of algorithms autonomously by processing datasets rather than being endowed and disciplined by humans.[18] Generally, this technology can be sorted into "supervised" and "unsupervised" ML, which is based on whether or not the processed data in the algorithm is labeled.[19] Additionally, there are advanced sub-categorized ML variants, such as reinforcement learning and deep learning.[20] The first refers to an ML technique where a contextual interrelation is adopted to train the algorithms to learn step–by–step to maximize the directional profit and the second is concerned with outperforming algorithmic skills to address a more complex cluster of datasets as large as ten million YouTube videos than the datasets for regular ML agents.[21] ML technology has proved to be successful in completing complicated tasks in diverse industries such as healthcare and transport, further showing great potential for broader application.[22] However, GDPR concerns can be triggered when data is collected and processed by the ML systems, especially when users are unaware that their personal information is being exploited by data controllers.[23] In consonance with the analysis of GDPR compliance in the ML environment, this article will later introduce three prominent ML sub-technologies with a high likelihood of raising GDPR issues.

---

18 SELECT COMMITTEE ON ARTIFICIAL INTELLIGENCE, AI IN THE UK: READY, WILLING AND ABLE? 2017–19, HL 100, ¶ 100 (UK).

19 Mircea-Constantin Scheau et al., *Artificial Intelligence / Machine Learning Challenges and Evolution*, 7 INT'L J. INFO. SEC. & CYBERCRIME 11, 12 (2018).

20 *See* Ulrich Schwalbe, *Algorithms, Machine Learning, and Collusion*, 14 J. COMPETITION L. & ECO. 568, 574–75, 577 (2018).

21 *See* Brian S. Haney, *The Perils and Promises of Artificial General Intelligence*, 45 J. LEGIS. 151, 160–63 (2018); Cody Weyhofen, *Scaling the Meta-Mountain: Deep Reinforcement Learning Algorithms and the Computer-Authorship Debate*, 87 UMKC L. REV. 979, 988 (2019).

22 THE ROYAL SOC'Y, MACHINE LEARNING: THE POWER AND PROMISE OF COMPUTERS THAT LEARN BY EXAMPLE 34 (2017), https://royalsociety.org/~/media/policy/projects/machine-learning/publications/machine-learning-report.pdf.

23 Stephen McJohn & Ian McJohn, *Fair Use and Machine Learning*, 12 NE. U. L. REV. 99, 153 (2020); GDPR, *supra* note 14, at 33.

1. Algorithms

The different ML sub-technologies, including supervised learning, unsupervised learning, reinforcement learning and deep learning, have been comprehensively applied in the algorithms.[24] They are also likely to be employed in business activities to analyze the large amount of data containing a high variety, velocity, and volume of information and to address different tasks specifically and separately.[25] Although the different ML sub-technologies' technical functions are similar to computer programs presenting some orders of calculation, similar results will come up if the imputed raw materials are highly relevant.[26] This explains why an algorithm can find information about idiosyncrasies within a data subject and use that to identify other data subjects who share similar characteristics.[27] This process is automatic because once algorithms have been trained with the so-called "training data" they will be "fully educated," which means that they can engage in processing other data without initial instructions, even if the other data is not distinguishable.[28]

Taking the algorithmic application in facial recognition as an example, as long as the programmer has imputed images of a person into the machine and told the machine that the image links to the face of that person, then the machine can automatically identify the same face if processing other images or selfies of the person.[29] However, algorithms do not produce the correct answer all the time, especially when hundreds of datasets are inserted into the unsupervised algorithms, producing questions as to which specific parts of an algorithm should be used and which are causing classification and clustering issues.[30] This is because, unlike the supervised learning, the imputed data is not labeled in the unsupervised machines, which indicates that the machines can autonomously and secretly make decisions about how to deal with the data.[31] Thus, the programmer cannot know how the data is classified or to check if the output derived from the data processing is correct or expected.[32] Similarly, algorithms

---

24 *See* Schwalbe, *supra* note 21, at 576–79.

25 *See id.* at 575–79.

26 *See* Warren E. Agin, *A Simple Guide to Machine Learning*, AM. BAR ASS'N (Feb. 16, 2017), https://www.americanbar.org/groups/business_law/publications/blt/2017/02/07_agin/.

27 *See* Harry Surden, *Machine Learning and Law*, 89 WASH. L. REV. 87, 90 (2014).

28 *See* Patrick W. Nutter, Comment, *Machine Learning Evidence: Admissibility and Weight*, 21 U. PA. J. CONST. L. 919, 930 (2019).

29 *Id.* at 930–31.

30 *See* Schwalbe, *supra* note 21, at 575; Nutter, *supra* note 29, at 935.

31 *See* Argyro P. Karanasiou & Dimitris A. Pinotsis, *A Study into the Layers of Automated Decision-Making: Emergent Normative and Legal Aspects of Deep Learning*, 31 INT'L REV. L. COMPUT. & TECH. 170, 173 (2017).

32 *See* Schwalbe, *supra* note 21, at 575.

with reinforcement learning properties aspire to maintain a long-term positive effect on a more stable analysis framework regardless of the short-term error costs.[33] Therefore, despite the uncertainties that ML algorithms will bring, their usage is basically warranted.

2. Data Hunting

Algorithms are rules for classifying or processing datasets, so a massive amount of data is essential to reach their most extensive efficiency. Also, as the United Kingdom Information Commissioner's Office (UK ICO) notes, a prerequisite for running ML systems is the accumulated datasets.[34] As the big data is defined as a great variety, velocity, and volume of grouped datasets, it demands the potent and intelligent information processing tools,[35] which can exhaust the full value of the datasets and process all data pieces.[36] The big data stores can be divided into Front-End databases and backup or archival databases, but these databases often partially choose tailored datasets to process and store instead of the entire big data.[37] In other words, although the data controller can scan and gather considerable data, only typical types of data will actually be processed and archived.[38] The so-called data summarization process has emerged many times, including in the scenario where the algorithm analyzes data from a behavioral and business perspective to tailor advertisements for specific customers respectively and to set prices that meet the customers' needs in different social stratifications.[39]

Moreover, big data analysis by ML has a wide range of benefits that are not only for individuals, but also for the community and society.[40] The utilization of big data can promote innovation, social interaction, economic efficiency, and

---

33 *See* Case C-507/17, Google v. Comm'n Nationale de l'Informatique et des Libertés, ECLI:EU:C:2019:772, ¶ 69 (Sept. 24, 2019); Schwalbe, *supra* note 21, at 576.

34 *See* INFO. COMM'RS OFF., BIG DATA, ARTIFICIAL INTELLIGENCE, MACHINE LEARNING AND DATA PROTECTION 7 (2017), https://ico.org.uk/media/for-organisations/documents/2013559/big-data-ai-ml-and-data-protection.pdf.

35 *Id.* at 6.

36 *Id.* at 11.

37 *See* Bernd Malle et al., *The Right to Be Forgotten: Towards Machine Learning on Perturbed Knowledge Bases*, *in* AVAILABILITY, RELIABILITY AND SECURITY IN INFORMATION SYSTEMS 251, 252–53 (F. Buccafurri et al. eds., 2016).

38 *See* Baharan Mirzasoleiman et al., *Deletion-Robust Submodular Maximization: Data Summarization with "the Right to be Forgotten"*, 70 INT'L CONF. ON MACH. LEARNING PROC. 2440, 2440 (2017).

39 *See* ORG. OF ECON. COOP. & DEV., ARTIFICIAL INTELLIGENCE IN SOCIETY 16 (2019), https://doi.org/10.1787/eedfee77-en.

40 *See* Jules Polonetsky & Omer Tene, *Privacy and Big Data: Making Ends Meet*, 66 STAN. L. REV. ONLINE 25, 28–29 (2013), https://review.law.stanford.edu/wp-content/uploads/sites/3/2016/08/PolonetskyTene.pdf.

even the efficacy of social governance.[41] This indicates that when grappling with data privacy concerns in the ML field, such as unauthorized or unjust collection, processing, and disclosure of personal data, and prejudicial treatment resulting from automated decision making,[42] these social or economic benefits can act as justifications for the action against data protection or data privacy. In addition, since the unsupervised learning has no humans in the loop and follows pre-designed models,[43] it is hard to predict the specific datasets it will use and to infer the outputs which may become new materials to be imputed in a new algorithmic process.[44] Similarly, the reinforcement learning exhibits the data analytical process that excludes human instructions, the same as unsupervised learning, although the so-called "trial-and-error" mechanism of reinforcement learning is different from the unsupervised counterpart.[45] This quality entails more flexible and broader access to external data for unsupervised or reinforcement ML agents irrespective of the data ownership and control and even a third party can access the data in virtue of data portability.[46] Again, some levels of data retention are necessary to keep the ML system functioning or to help fix the technical problems.[47]

3. Neural Networks

The ML organization of neural networks is in the propinquity to the topic of deep learning.[48] Although deep learning shares the same operating mechanism as other ML types which analyze data by algorithmic tools,[49] a network consisting of artificial neurons producing, delivering, and receiving the signals with special values in order to trigger the neurons to be activated stage by stage

---

41 *Id.* at 30.

42 *See* Sandra Wachter & Brent Mittelstadt, *A Right to Reasonable Inferences: Re-Thinking Data Protection Law in the Age of Big Data and AI*, 2019 COLUM. BUS. L. REV. 493, 506 (2019) (for instance, inferential analytics could collect and process indefinite amounts of data related to individuals and create biased outcomes based on the nuanced classification of these data).

43 *See* Case C-507/17, Google v. Comm'n Nationale de l'Informatique et des Libertés, ECLI:EU:C:2019:772, ¶ 69 (Sept. 24, 2019); Schwalbe, *supra* note 21, at 575.

44 Schwalbe, *supra* note 21, at 575.

45 *See* Rachel Wilka et al., *How Machines Learn: Where Do Companies Get Data for Machine Learning and What Licenses Do They Need?*, 13 WASH. J. L. TECH. & ARTS 217, 224–25 (2018).

46 *Id.* at 228–29.

47 *Id.* at 229–30.

48 *See* Case C-507/17, Google v. Comm'n Nationale de l'Informatique et des Libertés, ECLI:EU:C:2019:772, ¶ 56 (Sept. 24, 2019); Schwalbe, *supra* note 21, at 577.

49 Schwalbe, *supra* note 21, at 577.

is unique for deep learning.[50] As the learning process proceeds, the data passed on through the neuron connections will be slightly modified by each layer of neurons to adapt to the learning rules.[51] These neuron connections and the ways the neurons deal with data will also get changed based on the features of the data received.[52] The neurons in different layers are structured and connected as artificial nodes, which form a sophisticated and nuanced matrix.[53] The operation of the neuron networks often involves three types of deep learning techniques: supervised, unsupervised and reinforcement deep learning.[54] These neuron matrices are all complicated and intelligent but especially, the network of the reinforcement learning incorporates the so-called reward maximization process, which renders it more elusive than other networks.[55] Despite the fine configuration of the neurons, the three types of deep learning algorithms can still generate unpredictable results because either the machine cannot interpret some human language, or something goes wrong in the machine.[56] The unexpected decisions could also be made even though a deep learning machine with reinforcement property can be self-corrected by giving feedback on the authenticity of the result from the neurons at the output stage to the input and middle-stage neurons.[57] However, the deep learning algorithm with the neural network has been applied in many fields such as constructing complicated human languages including the interpretation of legal texts[58] and more remarkably, playing humanoid games such as the famous AlphaGo in the game Go.[59] In other words, deep learning systems have penetrated many spheres of our daily lives and processed numerous datasets related to personal information.

B. The Origin and Development of the Right to be Forgotten

The rise of Web 2.0 for the social interactive network has sped up the change of social recognition of remembering and forgetting by defining remembering

---

50 *See* Jürgen Schmidhuber, *Deep Learning in Neural Networks: An Overview*, 61 NEURAL NETWORKS 85, 86 (2015).

51 Schwalbe, *supra* note 21, at 577.

52 *See generally* Comm'n Nationale de l'Informatique et des Libertés, ECLI:EU:C:2019:772; Schwalbe, *supra* note 21, at 577.

53 Schwalbe, *supra* note 21, at 577.

54 *See* Karanasiou, *supra* note 32, at 173–74.

55 *Id.* at 173.

56 *Id.* at 174.

57 *Id.* at 174–75; *see generally* SELECT COMMITTEE ON ARTIFICIAL INTELLIGENCE, AI IN THE UK: READY, WILLING AND ABLE? 2017–19, HL 100 (UK); Weyhofen, *supra* note 22, at 989–90.

58 *See* Ilias Chalkidis & Dimitrios Kampas, *Deep Learning in Law: Early Adaptation and Legal Word Embeddings Trained on Large Corpora*, 27 A.I. & L. 171, 172 (2019).

59 Scott R. Granter et al., *AlphaGo, Deep Learning, and the Future of the Human Microscopist*, 141 ARCHIVES PATHOLOGY & LAB'Y MED. 619, 619 (2017).

as normality and forgetting as eccentricity.[60] Moreover, the next stage of Web 3.0 for the semantic web is in advent as the applications and programs are pervasively gathering data and purportedly sorting out and structuring specific data for personalization and contextualization, consequently causing the proliferation and dissemination of personalized data and deteriorating the value of forgetting.[61] The ML technology accelerates this process, as its characteristics enable the working of big data to create individual profiles according to each step people have taken online.[62] Web 4.0 which refers to the "symbiosis interaction between humans and machines" and the conceived Web 5.0 and 6.0, which herald more automated and intelligible machines equipped with potent and dynamic information analytics, are also approaching.[63] It seems that as technology advances, the utilization of information becomes widespread and vigorous, possibly rendering "forgetting" more unattractive.

However, due to technological achievements including extensive interconnection among intelligent agents, users' effortless accessibility to online publishing and omnipresent search engines, even one's naive mistake made in childhood sixty years ago can now be visible online.[64] Online intermediaries such as Google, Yahoo and Facebook have unprecedented power in everyday life concerning the usage and tracing of our personal information since they control a huge number of digital memories, possibly raising privacy concerns as a result.[65] Some arguments, such as "you are what Google says you are" and "Facebook Timeline feels like a privacy invasion to many because old information about us has not been recalled with ease or great detail in the past," epitomize the social demand to prevent digital memories from being revealed.[66] Hence, to protect one's data privacy, RTBF was accounted a fundamental right of EU citizens to request these online intermediaries and other data controllers/processors to throw away digital memories.[67]

---

60 VIKTOR MAYER-SCHÖNBERGER, DELETE: THE VIRTUE OF FORGETTING IN THE DIGITAL AGE 3–4 (2009).

61 Eugenia Politou et al., *Forgetting Personal Data and Revoking Consent under the GDPR: Challenges and Proposed Solutions*, 4 J. CYBERSECURITY 1, 10 (2018).

62 *See* George Bouchagiar, *Privacy and Web 3.0: Implementing Trust and Learning from Social Networks*, 10 REV. EUR. STUD. 16, 19–20 (2018).

63 Fernando Almeida, *Concept and Dimensions of Web 4.0*, 16 INT'L J. COMPUT. & TECH. 7040, 7041 (2017).

64 MAYER-SCHÖNBERGER, *supra* note 61 at 5.

65 *Id.* at 2, 6–7.

66 Meg Leta Ambrose, *You Are What Google Says You Are: The Right to be Forgotten and Information Stewardship*, 17 INT'L REV. INFO. ETHICS 21, 22 (2012).

67 *Id.* at 22–23.

1. The Landscape Before GDPR

The origin of RTBF can be traced back to a French or Italian right *droit à l'oubli* or *il diritto al'oblio* (the right to oblivion) that formerly offered ex-criminals the opportunity to remove their criminal records that were later no longer meaningful and valuable to the public.[68] This right implies that the prevention of personal information related to even criminal sentences from being linked with the individual's current status overtakes the value of the legitimate public accessibility to obsolete information.[69] Before the digital era, this right was usually associated with solving privacy issues regarding mass media production.[70]

However, since 1995, the EU has granted citizens a similar right to erase personal data as long as such data is illegally processed regardless of the substantial damage of privacy.[71] This right is valid unless there are contradictory rights or interests proved to be more overriding.[72] Also, the data controllers should erase all the personal data once requested because it is seen as a personal attribute under protection of the EU Charter of Fundamental Rights.[73] Directive 95/46/EC, the former regulation on data protection of the GDPR, states that data subjects have the right to "the rectification, erasure, or blocking of data that processing of which does not comply with the provisions of this Directive, in particular because of the incomplete or inaccurate nature of the data."[74] This right to erasure not only applies to the data controller but to the data processor as long as the controller has already erased the original data and notified the processor of this erasure with reasonable and proportionate efforts.[75]

The establishment of the right to erasure also involves Directive 2000/31/EC, which dictates that the online intermediaries are exempted from liability at the EU level to create a common European internal digital market.[76] In light of this,

---

68 *See* Aurelia Tamò & Damian George, *Oblivion, Erasure and Forgetting in the Digital Age*, 5 J. INTELL. PROP. INFO. TECH. ELEC. COM. L. 71, 72 (2014).

69 *See* Meg Leta Ambrose & Jef Ausloos, *The Right to Be Forgotten Across the Pond*, 3 J. INFO. POL'Y 1, 2 (2013).

70 Miquel Peguera, *The Right to Be Forgotten in the European Union*, *in* THE OXFORD HANDBOOK OF ONLINE INTERMEDIARY LIABILITY 486, 486 (Giancarlo Frosio ed., 2020).

71 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, art. 12(b), 1995 O.J. (L 281) 31, 42; Peguera, *supra* note 71, at 487.

72 Peguera, *supra* note 71, at 486–87.

73 *Id.* at 486; *see also* Charter of Fundamental Rights of the European Union, art. 8, 2012 O.J. (C 326) 391, 397.

74 Peguera, *supra* note 71, at 487.

75 *Id.* at 488.

76 *See* Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on Certain Legal Aspects of Information Society Services, in Particular Electronic Commerce, in the Internal Market (Directive on Electronic Commerce), art. 12, 2000 O.J.

the responsibility of preventing online infringement and protecting data rights of citizens falls on the national authorities because the national legal system can develop a unique framework of cyber regulation.[77] In 2012, the definition of the right to erasure was specified by Vivian Reding, the European Commissioner for Justice, Fundamental Rights, and Citizenship stating that the data, which bears any information concerning the data subject, should be removed from the system of the data controller without undue delay, unless there are outdoing legitimate grounds such as the freedom of speech.[78]

Other examples of exemptions under legitimate grounds from the right of erasure include "the processing of personal data carried out solely for journalistic purposes or the purpose of artistic or literary expression."[79] Third parties should be aware of the original deletion request of personal data, which indirectly asks the data controller to take "all reasonable steps" for the notification, unless this conduct is a "disproportionate effort."[80] This shows a balance between the legitimate objectives and privacy or personal dignity. The notion of dignity underpins the fundamental rights including privacy and data protection and depends on machine accountability, corporate compliance, and authorization of data subjects conceptualized as the principle of data protection.[81] Some scholars thus realize that the right to erasure represents a tough coordination between dignitary privacy and freedom of expression or public access to information.[82] Hence, the rule of the right to erasure comes up with such an expression.

(L 178) 1, 10.

77 *See generally* Michael J. Kelly & David Satola, *The Right to Be Forgotten*, 2017 U. ILL. L. REV. 1 (2017).

78 Robert Kirk Walker, Note, *The Right to be Forgotten*, 64 HASTINGS L.J. 257, 273 (2012).

79 *Id.*

80 *Id.*

81 *See* Anne de Hingh, *Some Reflections on Dignity as an Alternative Legal Concept in Data Protection Regulation*, 19 GER. L.J. 1269, 1275–76 (2018) (discussing how the European Union perceives human dignity as integral to the foundation of fundamental rights it seeks to protect).

82 Robert C. Post, *Data Privacy and the Dignitary Privacy: Google Spain, the Right to be Forgotten, and the Construction of the Public Sphere*, 67 DUKE L.J. 981, 990–92 (2018) ("The dignitary rights created by Article 7 of the Charter [of Fundamental Rights of the European Union] differ in important ways from the data privacy rights of Article 8 of the Charter. If the latter define and enforce proper bureaucratic handing of data, the former define and enforce social norms of respectful expression."); *see* Michael Douglas, *Questioning the Right to be Forgotten*, 40 ALT. L.J. 109, 109 (2015) ("Access to information on the open internet is 'essential' because it is the foundation of open discussion, and so plays an important function in democracies.").

2. GDPR Stipulations

As the legal practices and interpretations have furthered and enhanced the right to erasure in the past 20 years, Article 17 GDPR has inherited the essence of the old rules and slightly improved them.[83] Although there were earlier cases and legislative statements in Directive 95/46/EC, the right to erase/forget information had not been acknowledged as an independent data right until the enaction of the GDPR and court decision of *Google Spain.*[84] However, in GDPR, the phrase "right to be forgotten" is behind the right to erasure in the brackets regarding the word order, showing that the meanings of "erasure" and "forgotten" should be different.[85] The difference lies in the restrictive construction of the word "erasure" which only incorporates parts of the meaning of the word "forgotten".[86] In other words, compared to the mere "information erasure", there are manifold approaches for cyber society to "forget" one's personal information and prevent further dissemination in the digital context, such as anonymization, delisting search results, and changing the context of the information.[87] However, in contrast to the "erasure", some academics see these new approaches as independent measures that cannot be cohesively defined because they entail different requirements and standards to data controllers and processors.[88]

In addition, similar to Reding's interpretation of the right to erasure, GDPR requires controllers to inform other controllers which utilize personal data by exhausting reasonable efforts.[89] The statute also prescribes the exceptions to this right regardless of the grounds that the first subclause of Article 17 outlines.[90] Meanwhile, Article 18 underlines the circumstances where data should be restrictively processed instead of erased and thus offers an alternative way to

---

83 *See* GDPR, *supra* note 14, at 31.

84 Council Directive 95/46, art. 12, 1995 O.J. (L 281) 31 (EC); *See* GDPR, *supra* note 14, at 24; Case C-131/12, Google Spain SL v. Agencia Española de Protección de Datos, ECLI:EU:C:2014:317, ¶¶ 97–99 (May 13, 2014); Francesco Di Ciommo, *Privacy in Europe After Regulation (EU) No 2016/679: What Will Remain of the Right to Be Forgotten?*, 3 ITALIAN L.J. 623, 623–24 (2017).

85 Ciommo, *supra* note 85, at 624–25.

86 *Id.* at 625 n.6.

87 *See id.* at 625–26.

88 *See* Justin Kwik, *In the Light of the Technical Impracticality of the Right to Erasure, What Answers Can Actor-Network Theories Provide?*, 2019 SING. COMP. L. REV. 48, 48–49 (2019) ("Although some authors interpret the 'right to erasure' as simply having the same powers as the right to de-listing, albeit with a larger scope, this essay concurs with the Article 29 Working Party, Ambrose, Bunn and Graux in stating that it is imperative not to conflate these two separate rights, as they have accord drastically different obligations and implications, especially in today's digital environment.").

89 *See* GDPR, *supra* note 14, at 31.

90 *See id.*

address RTBF issues.[91] What Article 18 stipulates could also be considered as an alternative to the erasure if the data subject repudiates the deletion of personal data used for illegal processing according to Article 17(1)(d), but expects to keep the data archived for the sake of their interests.[92] Although the data is still stored, the limitations of the processing could become very strict.[93] Overall, the language of RTBF in GDPR implies an obligation for data controllers and third parties which entails the removal of the information or other approaches to expeditiously "forget" the information in the whole cyberspace under justifiable requests.[94] However, some terms, such as the word "reasonable," still lack explanatory clarity, possibly causing loopholes and confusion when applying these rules in specific situations.[95] The consistency between the legislation, case law, and the freedom of expression remains controversial.[96]

3. Case Studies

Since the enactment of Directive 95/46/EC, there have been numerous cases about RTBF and its forerunner the right to erasure.[97] One of them is the landmark case of *Google Spain*.[98] The case involves a Spanish citizen Mario Costeja, whose data right was infringed by Google Search results linking to a newspaper advertisement published in 1998 and recording a debt he owed.[99] Because this debt information was already outdated, the search result caused significant damage to his career.[100] He then brought a petition before the Spanish Data

---

91 GDPR, *supra* note 14, at 31–32. *See* Amanda Cheng, *Forget About the Right to Be Forgotten: How About a Right to Be Different?*, 22 AUCKLAND U. L. REV. 106, 135 (2016).

92 *See* Gloria González Fuster, *Article 18. Article 19*, *in* THE EU GENERAL DATA PROTECTION REGULATION (GDPR): A COMMENTARY 485, 489–90 (Christopher Kuner et al. eds., 2020).

93 *Id.* at 487.

94 *See* Eugenia Politou et al., *Backups and the Right to Be Forgotten in the GDPR: An Uneasy Relationship*, 34 COMPUT. L. & SEC. REV. 1247, 1248–49 (2018).

95 *See* Akriti Gupta & Mahima Sharma, *Data Privacy in Digital World: Right to Be Forgotten*, 8 NIRMA U. L.J. 97, 107 (2018); *see generally* GDPR, *supra* note 14; Cheng, *supra* note 92 at 134.

96 *See* Bouchagiar, *supra* note 63, at 25; *see also* Michael L. Rustad & Sanna Kulevska, *Reconceptualizing the Right to Be Forgotten to Enable Transatlantic Data Flow*, 28 HARV. J.L. & TECH. 349, 371–72 (2015); Ambrose & Ausloos, *supra* note 70, at 12.

97 *See* GDPR, *supra* note 14, at 2.

98 Case C-131/12, Google Spain SL v. Agencia Española de Protecci6n de Datos, ECLI:EU:C:2014:317, ¶ 1 (May 13, 2014).

99 *See* Ana Azurmendi, *Spain: The Right to Be Forgotten*, *in* PRIVACY, DATA PROTECTION AND CYBERSECURITY IN EUROPE 17, 22 (Wolf J. Schünemann & Max Otto Baumann eds., 2017).

100 *Id.*

Protection Agency (SDPA).[101] However, the SDPA denied his request to remove the information from the newspaper and instead asked Google to delist the indexes related to his debt.[102] Google declined to de-index and brought litigation against the agency before the Spanish National High Court, which later became a proceeding of the European Court of Justice (CJEU) because of the necessity to interpret Directive 95/46/EC.[103]

First, the court recognized Mr. Costeja and Google Spain, together with its parent company Google Inc., as data subjects and controllers.[104] Second, CJEU claimed that since the reasons and purposes to process the information had disappeared, even a re-use of personal data by the controller could be an invasion of privacy without showing any substantial loss from privacy infringement.[105] Therefore, according to the law then applied, it was evident that Google must implement the right to erasure due to a lack of purposes for processing.[106] The Spanish High Court and the CJEU found an alternative way to "forget" by removing the relationship between Costeja's name and the questioned information and delisting the search result URLs.[107] This case sets out a benchmark for search engines, which indicates that delisting the search results can be a feasible way to apply the right to erasure or RTBF because it seems impossible to delete all the relevant datasets in cyberspace, or *a fortiori*, in the ML scenarios.[108] Also, search engines need to contemplate the balance of interests regarding each specific request to delete the URLs in order to confirm the righteousness of their next action to retain or delete.[109]

Another prominent case related to Google is *NT1 and NT2*, where the two applicants were treated differently because their previous criminal offenses were of diverse seriousness and different public influence.[110] The court rejected to delist the first claimant's criminal record of false accounting to evade tax because this action was considered as his habitual behavior, but the court agreed with the second claimant's request to delist because he committed minimal wrongdoing of computer hacking which was irrelevant to his future performance.[111] Additionally, how to request the primary online publishers to

---

101 *Id.*

102 *Id.*

103 Google Spain SL, ECLI:EU:C:2014:317, ¶¶ 15, 18; Ciommo, *supra* note 85, at 638–40.

104 Google Spain SL, ECLI:EU:C:2014:317, ¶ 43.

105 *See* Peguera, *supra* note 71, at 490; Post, *supra* note 83, at 998.

106 Julia Powles, *The Case that Won't Be Forgotten*, 47 LOY. U. CHI. L.J. 583, 587 (2015).

107 *Id.* at 588.

108 *Id.* at 588–91.

109 *See* Bouchagiar, *supra* note 63; Peguera, *supra* note 71, at 491.

110 Peguera, *supra* note 71, at 492–93.

111 *Id.* at 493.

"forget" the information was appraised by national courts and the European Court of Human Rights (ECHR).[112] The courts have developed various ways including anonymizing the name, and de-indexing the content in the search result page, but rarely asked for the complete deletion of the whole publisher's archives.[113] To conclude, the measures in the case law to forget digital memory vary and yet it lacks a unified standard to apply the law.

II. PROBLEMS TO APPLY RTBF AGAINST THE MACHINE LEARNING BACKGROUND

Under GDPR and the relevant case law, RTBF in a way symbolizes the self-determination of personal information.[114] Self-determination refers to the independent individual decision on whether, how, and to what extent the data subject presents himself/herself to others or the public. If the personal information is under the data subject's control, he/she can make such a decision.[115] Together with the value of dignity and the individual autonomy it reflects, self-determination somehow shapes the notion of democracy as the values entail the separation of societal sub-systems and can realize self-reliant conversation without undue or biased interventions.[116] RTBF partly provides the opportunity of self-determination as data subjects can at least freely delete the information that they do not wish to be revealed or re-used. At the same time, this right creates alternative options for search engines and online service providers to "forget" instead of merely erasing the whole content, ostensibly adding more flexibility to apply RTBF. However, the language of "forgetting" in Articles 17, 18 and 19 is vague, especially when describing how to reasonably "forget" and how to notify others of the request, consequently inducing legal uncertainty to the application.[117] Furthermore, this situation of application may be worse in the ML context. This is because the algorithms, the primary driver of the ML system, could hunt data as much as possible, leading to an unrestricted extension of digital memories that can hardly be "forgotten" completely.

---

112 *See generally* Hurbain v. Belgium, App. No. 57292/16 (June 22, 2021), https://hudoc.echr.coe.int/fre?i=001-210884.

113 *See generally id.*

114 *See* Giancarlo F. Frosio, *The Right to be Forgotten: Much Ado about Nothing*, 15 COLO. TECH. L.J. 307, 309–11, 313 (2017).

115 *See* Virginia Kozemczak, *Dignity, Freedom, and Digital Rights: Comparing American and European Approaches to Privacy*, 4 CARDOZO INT'L & COMP. L. REV. 1069, 1073 (2021).

116 *See* Gerrit Hornung & Christoph Schnabel, *Data Protection in Germany I: The Population Census Decision and the Right to Informational Self-Determination*, 25 COMPUT. L. & SEC. REV. 84, 85–86 (2009).

117 *See* GDPR, *supra* note 14, at 31–32; Cheng, *supra* note 92, at 134.

Additionally, the process of remembering and forgetting in the algorithm varies from the non-algorithmic counterparts and increases the difficulty in implementing RTBF.[118] It is doubtful whether the current legislative approaches presented by GDPR and the case law really work or whether new approaches should be embraced.[119]

A. Lack of Guidance of the Laws

A prominent lacuna in the legal text is that there is no clear definition of how to virtually "forget" digital memory or ML agents. Admittedly, there is some guidance, including guidelines issued by the European Data Protection Board (EDPB) and case law related to the operation and response to requests to delist results in search engines and how the grounds for and against de-indexing have been weighed and balanced..[120] However, it is suspicious that this guidance tailored to search engines in the conventional cyberspace landscape can be smoothly applied against an ML backdrop as the machinery environment comprises unique and dynamic characteristics.[121] Online content publishers probably deserve a different way of "forgetting" *vis-à-vis* the search engines. A lack of standards could nevertheless trigger diverse RTBF approaches.

1. The GDPR Text

Article 17 of GDPR lists conditions for obligatory erasure and exceptions that strike a balance between privacy (dignity) and the public right to information (freedom of expression). The provision also delineates the scope of the deletion, which applies to all data controllers and processors, as well as the obligation of reasonable efforts to inform other parties of data controllers, but it lacks detailed examples or standardized prescriptions on conduct.[122] Meanwhile, Article 19 of the GDPR maintains that controllers do not need to contact all the publishers who have disclosed the data at issue if this communication is impossible or the effort is disproportionate.[123] Correspondingly, controllers and processors will

---

118 Elena Esposito, *Algorithmic Memory and the Right to be Forgotten on the Web*, 4 BIG DATA & SOC'Y 1, 2 (2017).

119 *See generally* Antonio A. Ginart et al., *Making AI Forget You: Data Deletion in Machine Learning*, *in* 32 ADVANCES IN NEURAL PROCESSING SYSTEMS (2019).

120 *See generally Guidelines 5/2019 on the Criteria of the Right to be Forgotten in the Search Engines Cases Under the GDPR (Part 1)*, EUR. DATA PROT BD. (July 7, 2020), https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-52019-criteria-right-be-forgotten-search-engines_en.

121 Mario Martini, *Regulating Artificial Intelligence – How to De-Mystify the Alchemy of Code?*, *in* ALGORITHMS & LAW 103–04 (Martin Ebers & Susana Navas eds., 2019).

122 GDPR, s*upra* note 14, at 12.

123 *Id.* at 32.

likely be uncertain whether their actions to "forget" data will be within RTBF compliance or whether the forgetting approaches are enough to enforce RTBF.[124]

As a result, some scholars argue that the EU official goal of data protection is to promote the data analysis and to create a considerable amount of revenue from it.[125] From the perspective of the ML algorithm, which is inherently imbalanced and discriminative to certain social groups, such blurry language may consequently aggravate this inequality by prejudicial interpretation of the GDPR itself and by treating different social groups with differential "forgetting" measures according to the predictions of how to maximize profits.[126] Therefore, in the context of ML where algorithms and big data would be deployed comprehensively, it is hard to imagine that data controllers will accurately understand the authentic meaning of effective "forgetting."[127] Without a universal standard, these controllers will hardly give up their interests in making huge profits, rather than focusing on the vaguely sufficient realization of RTBF when processing big data.[128]

2. Practical Instructions

There are a few practical codes issued by different institutions about how and when to apply the RTBF concretely. The EDPB guidelines introduce the legal rationales for data subjects to ask for delisting and describe the grounds to delist or to take down URLs individually, but do not mention any substitutable schemes to delist.[129]

Similarly, the UK ICO has formulated a guideline on how to apply GDPR (including RTBF as a right therein) consistent with UK Data Protection Act 2018.[130] The guideline states that notification of erasure should be drawn to other organizations who have received the concerned data and should be delivered to

---

124 *See* Politou, *supra* note 62, at 1249.

125 *See* Tal Z. Zarsky, *Incompatible: The GDPR in the Age of Big Data*, 47 SETON HALL L. REV. 995, 1003 (2017).

126 Bryce Goodman & Seth Flaxman, *European Union Regulations on Algorithmic Decision Making and a "Right to Explanation"*, 38 A.I. MAG. 50, 53 (2017).

127 *See* Polonetsky, *supra* note 41; *see also* Wilka et al., *supra* note 46, at 221–22; Villaronga et al., *supra* note 13, at 311, 313. *See generally* International Conference of Data Protection & Privacy Commissioners, *International Resolution on Privacy as a Fundamental Human Right and Precondition for Exercising Other Fundamental Rights* (Oct. 21–24, 2019).

128 *See generally* A & B v. Ediciones El Pais, ECLI:ES:TC:2018:58 (June 4, 2018); Zarsky, *supra* note 126.

129 *See* Ginart et al., *supra* note 120, at 3–4.

130 *See* INFO. COMM'RS OFF., *supra* note 35, at 9.

the data subject unless the effort is unreasonable in that the data has been disclosed to the public or other private parties.[131] It also prescribes that whether the data should be deleted from the archive depends on the mechanical and schedule availability of the data controllers/subjects.[132] It additionally mentions several "forgetting" steps such as overwriting the backup retention which replaces the backup contents with other information in light of an established agenda and other methods in order to render the data "beyond use."[133] This practical guide is speciously effective in addressing RTBF issues more flexibly but as mooted by Villaronga et. al., these approaches could still be insufficient and tentative for the application of RTBF in ML agents.[134]

Likewise, after *Google Spain*, the Article 29 Data Protection Working Party (Working Party, now the EDPB Board) has given some tips on how to implement RTBF practically in search engines.[135] The Working Party Guideline maintains that the data subjects' requests should be considered circumspectly by European Data Protection Authorities (DPAs) and there is no need for original publishers to delete the related content or to communicate with the search engines and the subjects.[136] In addition, except for some particular circumstances, the delisting result does not need to be publicized.[137] This guideline is basically the same as the EDPB Guideline in terms of addressing GDPR requests and still lacks a specific standard for ML-based RTBF.

The above institutional instructions, aside from the forgetting measures proposed by them that are rarely exercisable in practice, are short of legally-binding force as they are likely to be regarded as "soft law" and their legal validity to discipline all the actors is under suspicion.[138] For example, even if EDPB is distinct from the advisory function of the Working Party, this organization can only play a secondary role in enforcing GDPR compared to national data protection authorities,[139] let alone its non-binding guidelines. This, reflects that these quasi-legislative documents are also unable to address RTBF

---

131 *Id.* at 108.

132 *Id.* at 118.

133 *Id.*

134 *See generally* International Conference of Data Protection & Privacy Commissioners, *supra* note 10; *see also* Villaronga et al., *supra* note 13, at 311.

135 *See generally* Article 29 Data Protection Working Party, *Guidelines on the Implementation of the Court of Justice of the European Union Judgment on "Google Spain and Inc. v. Agencia Espanola de Proteccion de Datos (AEPD) and Mario Costeja Gonzalez" C-131/21* (Nov. 26, 2014), https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=667236.

136 *Id.* at 2.

137 *Id.* at 12.

138 Jaap Hage, *What Is Legal Validity? Lessons from Soft Law*, *in* LEGAL VALIDITY AND SOFT LAW 19, 20 (Pauline Westerman et al. eds., 2018).

139 Christina Etteldorf, *EDPB on the Interplay Between the ePrivacy Directive and the GDPR*, 5 EUR. DATA PROT. L. REV. 224, 225 (2019).

issues.

3. The Case Law

The cornerstone case *Google Spain* and the case *NT1, NT2* seem to have determined the definition of the way to "forget" and deliberated about the reasons to delist the indexes related to one's name or other outdated personal information. In the past several years, there has been a vast number of requests to delist the related URLs for miscellaneous reasons, though the above two take a large portion.[140] Thus, it seems that delisting URLs from search results has been a *modus operandi* for data controllers to implement the RTBF. However, as the scope of this right does not differentiate between requesters, if the controller uses interrelated and intricate systems of ML to process data, a mere action of delisting URLs related to an individual by search engines could cause harm to other persons' digital memory and the machine cannot reach the status of completely forgotten.[141] This is because the URLs requested to be de-indexed may direct to a webpage containing other's information, and if the de-indexing conduct has been done, the individual who shares the information on the same website cannot access the de-indexed page.[142] To the contrary, as the sourced data still exists, the algorithms are able to skim all the data and sift those closely pertinent out from the dense datasets to process without directly tracing the particular information.[143] Accordingly, the benchmark for delisting action shown in the related cases will be problematic.

Another category of case ruling is the RTBF approach for online publishers. One of the most notable cases is *M.L. and W.W. v. Germany* where the claimants tried to anonymize their names in a media report related to their conviction of murder and were nevertheless rejected by the German Federal Court of Justice and ECHR.[144] This anonymization approach could be another way of applying RTBF since the German authority and the ECHR have considered this measure to be workable,[145] although the two plaintiffs failed in this case due to the overriding importance of publication interest.[146] Despite this consideration, it is

---

140 Theo Bertram et al., *Five Years of the Right to be Forgotten*, *in* 2019 ACM SIGSAC CONFERENCE ON COMPUTER AND COMMUNICATIONS SECURITY (CCS'19) 959, 963 (2019).

141 Powles, *supra* note 107, at 587–88; Esposito, *supra* note 119, at 3.

142 Esposito, *supra* note 119, at 3.

143 *Id.* at 4.

144 M.L. & W.W. v. Germany, App. Nos. 60798/10 & 65599/10, ¶ 12 (June 18, 2018), https://hudoc.echr.coe.int/app/conversion/docx/pdf?library=ECHR&id=001-183947&filename=CASE%20OF%20M.L.%20AND%20W.W.%20v.%20GERMANY.pdf.

145 *Id.* ¶¶ 76, 105.

146 *Id.* ¶ 116.

still uncertain if anonymization tools can work practically and sustainably when facing the ML context.[147]

B. The Paradox of Practically Forgetting

To push ahead of the points of the dearth of the above legal effectiveness concerning RTBF and the ML environment, it is vital to explore the practical obstacles to precisely apply this right through alternative technical measures other than the mere "erasure" to "forget" in the ML context.[148] This is mainly due to the fact that "data deletion requirements can be considered to actually border on the edge of impossibility[,]"[149] which means numerous technical and operational problems could exist when RTBF and ML systems are intertwined.[150] Meanwhile, it is difficult to pick out the most effective way to solve technical issues of RTBF implementation in line with the related construction in GDPR, which is doctrinally considered as the benchmark.[151]

At the same time, in the digital era, it seems to be more effortless and costless to remember but increasingly tricky and lavish to forget.[152] By aggregating those "data memories," the industrial production will be more efficient and cyberspace regulation be more precise.[153] However, the usage of the compact information aggregations could also cause severe damage and errors that even erode the welfare it generates.[154] A mere cost-effective analysis is deficient to meet the nuanced needs in different scenarios.[155] Thus, it is necessary to rebalance the grounds for forgetting and for remembering such as public or economic interests. In sum, the practical conundrum of forgetting, paired with the improper distribution of the rights and obligations concerning the implementation of forgetting measures, and the intense debate between the fundamental value for and against RBTF creates a forgetting paradox.[156]

1. It is Nearly Impossible to "Forget" All Digital Memories

Due to the features of ML technology and the legal requirements to implement RTBF, not only the measure of erasure, but also other alternative means of

---

147 *See* International Conference of Data Protection & Privacy Commissioners, *supra* note 10; Villaronga et al., *supra* note 13, at 310.
148 Villaronga et al., *supra* note 13, at 316.
149 *Id.* at 305.
150 Kwik, *supra* note 89, at 56.
151 Villaronga et al., *supra* note 13, at 309.
152 MAYER-SCHÖNBERGER, *supra* note 61, at 92.
153 *Id.* at 93–94.
154 *Id.* at 95–96.
155 *Id.* at 96.
156 *See* discussion *infra* Sections 3.2.1, 3.2.2, 3.2.3.

"forgetting" may prove to be futile to effectively forget all the digital memories in the ML context.[157] These two approaches jointly signify the inadequacy of the current legal framework, even by its extensive interpretation, to achieve an expected application of this right on the data-driven and algorithmic basis.[158]

It may be nearly impossible to completely delete or block all access to the data or digital memories regarding AI agents.[159] To achieve full "forgetting" data controllers and processors must (1) continuously trace all the digital locations where the relevant data, including the derivative data is archived, and (2) individually evaluate whether the data should be deleted or de-indexed within a reasonable period of time, but doing so is costly.[160] After the tracing and evaluation, the data at issue should be removed from the requester's view to prove it has been forgotten.[161]

Even if an outdated document has been deleted as a result of the exercise of RTBF, the algorithms can still restore and reproduce the entire contents of that document in that they can collect and process the adjacent records in the file stock.[162] The algorithms can also scan or sort out large information clusters by virtue of their humanoid and intelligent neuron networks as well as the reinforced self-learning technology.[163] However, if the deletion of contiguous information is unattainable, it seems that the mere erasure of the information at issue is obviously not enough to attain the purpose of RTBF.[164] Specifically, the data records are stored in various databases and are searched out by clicking the indexes on the user-computer interface rather than by direct screening by users, generating a high standard of functioning requirements called atomicity, consistency, isolation and durability and raising practical obstacles to delete or overwrite all the relevant databases as these actions will harm the stability.[165]

While the routine performance to erase the data in an ML agent is to cut down the index connection between the neuron dots in the algorithm network, there is currently no succinct benchmark on how to disconnect the index practically.[166]

---

157 *See* Villaronga et al., *supra* note 13, at 310.

158 *See* HELENA U. VRABEC, DATA SUBJECT RIGHTS UNDER THE GDPR 156–158 (Oxford Univ. Press 2021).

159 *See id.* at 158.

160 *See* Chris Prince et al., *The Aleph Bet: Debating Metaphors for Information, Data Handling and the Right to Be Forgotten*, 16 CAN. J. L. TECH. 171, 173–74 (2018).

161 *Id.* at 174.

162 *See* Sajam Garg et al., *Formalizing Data Deletion in the Context of the Right to be Forgotten*, *in* ADVANCES IN CRYPTOLOGY – EUROCRYPT 2020 373, 376 (Anne Canteaut & Yuval Ishai eds., 2020).

163 *See* Kwik, *supra* note 89, at 50, 62.

164 GDPR, *supra* note 14, at 32.

165 Villaronga et al., *supra* note 13, at 308–09.

166 *Id.* at 309–10.

Likewise, for some databases which deal with the "data fragments" statistically, even a limited data erasure could trigger the reconstruction of the whole database.[167] This indicates the impossibility of deleting data upon one's request if the algorithm extracts data from these databases.[168] The data can be re-traced by the algorithms if the new network is rebuilt.[169]

The data deletion may interrupt the consistent functioning of a particular ML process. Regarding long-term backups, which store the long history of the previous algorithmic processing as references for future operation and possess extraordinary merits for the consistency of the ML process, a certain level of deterioration of such backups could negatively affect the entire operation of the machine.[170] Concurrently, the efficiency of the algorithm could decrease due to a lack of data of enough volume, possibly resulting in the ineffectiveness of the whole ML process.[171] Accordingly, the arbitrary choice between the mere deletion of specific data and delisting indexes is likely to be very harmful to the running and ability of the ML system, and thus inappropriate for the application of RTBF. [172]

Furthermore, new technical measures, such as encryption, anonymization and pseudonymization are still not as effective as they are presumed to be.[173] For instance, while the machines can process the encrypted data without decryption through the so-called "functional encryption" preserving the merit of RTBF, the current algorithms are still inefficient to deal with the data if its size is too large.[174] Even if the algorithms are competent to process large datasets, problems still exist related to the latent manipulation of open data by data controllers or third parties and the security of the "data keys."[175]

Anonymization and pseudonymization approaches share a similar shortcoming that they are currently not very serviceable.[176] This is due first to the immaturity of these measures or the de-anonymizing tools to decode the encrypted data, inducing the re-matching of specific personal information.[177]

---

167 Malle et al., *supra* note 38, at 253.

168 *Id*.

169 ROYAL SOC'Y, *supra* note 23 at 20.

170 Politou et al., *supra* note 95, at 1251.

171 Dimitra Kamarinou et al., *Machine Learning with Personal Data*, 247 QUEEN MARY UNIV. OF LONDON, SCH. OF L. 1, 14 (2016) https://ssrn.com/abstract=2865811.

172 Kwik, *supra* note 89, at 56.

173 Villaronga et al., *supra* note 13, at 310.

174 *Id.*

175 PETER DRUSCHE ET AL., THE RIGHT TO BE FORGOTTEN – BETWEEN EXPECTATIONS AND PRACTICE, ENISA-EUROPEAN UNION AGENCY FOR CYBERSECURITY 11–12 (2011) https://www.enisa.europa.eu/publications/the-right-to-be-forgotten.

176 Villaronga et al., *supra* note 13, at 310.

177 *See* McKay Cunningham, *Privacy Law That Does Not Protect Privacy, Forgetting the Right to Be Forgotten*, 65 BUFF. L. REV. 1, 16 (2017).

Second, the scope of "personal data" tends to be insulated from the cryptic data, as the definition of "personal data" in GDPR involves the data related to an identified or identifiable person to which at least the anonymized data does not belong.[178] Although pseudonymized data ostensibly falls inside the ambit of "personal data" as GDPR asks for all reasonable steps to re-identify the data subject, it is still unknown of the scope of "reasonable means" articulated in Recital 26 and it seems that not all pseudonymized data could be de-coded with proportionate efforts.[179] Thus, the encrypted data probably falls outside the definition of the personal data according to *Breyer*.[180] Hence, it is possible that if the personal data is encrypted, the RTBF as a GDPR right will lose its effect.[181] The delinking approaches that render the personal information amongst datasets inaccessible by concealing or falsifying the personal identification indexes are unlikely to be workable as well. This is because if the data controller uses advanced algorithms and synthesizes several large databases for the algorithmic profiling, the anonymized or pseudonymized data could be decrypted, making the data relink to an identifiable individual.[182] The decrypted data thus comes within the scope of the "personal data" in GDPR.[183]

Therefore, although GDPR requires extra safeguards added to the de-identification methods, which is supposedly promising,[184] the encrypting, anonymizing, and pseudonymizing measures still cannot disable all the data linkage with personal identities.[185] Since the current approaches to delete or block access to all the data could trigger technical errors and system damage,[186] it is better to find new ways to apply this right under the appropriate interpretation of the GDPR, the relevant guidance and the case law.

---

178 *See id.* at 12; *see also see also* Lee A. Bygrave et al., *Personal Data*, *in* THE EU GENERAL DATA PROTECTION REGULATION: A COMMENTARY 22, 22 (Christopher Kuner, Lee A. Bygrave & Christopher Docksey eds. 2020).

179 David Peloquin et al., *Disruptive and Avoidable: GDPR Challenges to Secondary Research Uses of Data*, 28 EUR. J. HUM. GENETICS 697, 699 (2020).

180 Case C-582/14, Patrick Breyer v. Bundesrepublik Deutschland, ECLI:EU:C:2016:779, ¶ 46 (Oct. 9, 2016).

181 Gerald Spindler & Philipp Schmechel, *Personal Data and Encryption in the European General Data Protection Regulation*, 7 JOURNAL OF INTELL. PROP., INFO. TECH. AND E-COM. L. 163, 176–77 (2016).

182 Ira S. Rubinstein & Woodrow Hartzog, *Anonymization and Risk*, 91 WASH. L. REV. 703, 713 (2016).

183 *See* GDPR, *supra* note 14, at 24.

184 Elizabeth A. Brasher, *Addressing the Failure of Anonymization: Guidance from the European Union's General Data Protection Regulation*, 2018 COLUM. BUS. L. REV. 209, 232–233, 248–49, 251, 253.

185 Sophie Stalla-Bourdillon & Alison Knight, *Anonymous Data v. Personal Data – A False Debate: An EU Perspective on Anonymization, Pseudonymization and Personal Data*, 34 WIS. INT'L L. J. 284, 298, 301 (2016).

186 Kwik, *supra* note 89, at 51.

2. An Incomplete Blend of Rights and Obligations Related to RBTF Enforcement

Regardless of the above technical inability to exercise RTBF and the absence of a direct definition, GDPR also lacks explicit and all-around rules regarding the multilayered operational and obligatory guidance for data controllers, processors and third parties at different stages, which could encroach on the effectiveness of RBTF in some cases.[187] This concern is first related to the GDPR obligations for the third-party controllers.[188] Article 17 (2) GDPR states that apart from the data controllers being directly requested, only third parties which have been informed by these controllers need to erase the related links, copies, and replications.[189] This provision also mentions an ambiguous norm of "reasonableness". These issues may provoke various interpretations and multiple applicable approaches of RTBF before reviewing by data protection agencies and the courts.[190] For search engines, although *Google Spain* has set forth an example for Google as the data controller (being requested to remove the related hyperlinks), it is still unknown if other search engines need to take the same action as well.[191] This is because Article 17 (2) GDPR solely calls for the reasonable endeavors to the greatest magnitude of data controllers at the forefront to inform other parties who have indirectly collected the relevant data but lacks the stipulation of subsequent actions for these third-party controllers (search engines).[192]

In a more complicated case, where some search engine operators have legitimate grounds for derogations enumerated in the third paragraph of Article 17 while others do not have, it is still unpredictable if the third-party operators will choose to de-reference the relevant information or not.[193] This is either because the third-party engines have not been notified or it is unclear who is in

---

187 The ruling of Google Spain does not clearly allocate the responsibilities to enforce RTBF between search engines such as Google and website publishers. Also, the text of GDPR and its guidance provide incomplete instructions thereon. HERKE KRANENBORG, ARTICLE 17. RIGHT TO ERASURE ('RIGHT TO BE FORGOTTEN') IN: THE EU GENERAL DATA PROTECTION REGULATION (GDPR) 475, 479 (Christopher Kuner et al. eds., 2020).

188 *See infra* discussion and accompany notes 190–97.

189 Alessandro Mantelero, *The EU Proposal for a General Data Protection Regulation and the Roots of the 'Right to be Forgotten'*, 29 COMPUT. L. & SEC. REV. 229, 238 (2013); Giovanni Sartor, Fac. of L., Eur. Univ. Inst. Florence, The Right to Be Forgotten in The Draft Data Protection Regulation, 71, 75, 79 (Oct. 28, 2014).

190 Mantelero, *supra* note 190.

191 Stefania Alessi, *Eternal Sunshine: The Right to Be Forgotten in the European Union after the 2016 General Data Protection Regulation*, 32 EMORY INT'L L. REV. 145, 164 (2017).

192 *Id.*

193 *See* Cesare Bartolini & Lawrence Siry, *The Right to Be Forgotten in the Light of the Consent of the Data Subject*, 32 COMPUT. L. SEC. REV. 218, 229–30 (2016).

charge of the de-indexing action in specific circumstances, which will finally cause different outcomes of index removal among third-party search engines in practice.[194] Evidently, Google has been under the spotlight of exercising RTBF due to an immense number of requests to delist the URLs[195] and the involvement in many corresponding litigations such as *Google Spain, NT1, NT2* and *Google v. CNIL*. Other online service providers should not be ignored as they could also receive delisting requests or act pre-emptively to avoid repetitive deletion concerning the link to the same content.[196] However, whether to take action to inform or not is still at the discretion of the third-party search engines, but GDPR does not provide any clear criteria for them to follow.[197]

Secondly, this legislative defect can be amplified in the scenarios of the extraterritorial application of RTBF to avoid the collection of the questioned data from states outside the EU.[198] The CJEU in *Google v. CNIL* claimed that the delisting requirement did not apply in jurisdictions that had no laws on the de-referencing action or the general RTBF rules, in parallel with the conclusion of the French Data Protection Authority.[199] Against the ML backdrop, the ineffectiveness of the obligatory delisting action is possibly aggravated.[200] This is because the machines can sort out fragmented but useful information by algorithms from the processing of a large volume of data, as exemplified by the algorithmic application in the language interpretation.[201] Consequently, web contents with their URLs removed can be re-linked by redirecting to search results derived from other search engines in other languages or located in cyberspaces of other states, which signifies the incomplete "forgetting."[202] Some retort that the problem of relinking to foreign sources could be mitigated by the so-called "geo-blocking" which demands delisting all the relevant URLs based on the location of the searchers.[203] Google also offered this solution in its

---

194 *Id.*

195 GOOGLE, *Requests to Delist Content Under European Privacy Law*, GOOGLE TRANSPARENCY REPORT, https://transparencyreport.google.com/eu-privacy/overview, (last visited Jul. 8, 2020).

196 Alessi, *supra* note 192, at 170–71.

197 *Guidelines 5/2019 on the Criteria of the Right to Be Forgotten in the Search Engines Cases Under the GDPR (Part 1)*, EUR. DATA PROT. BD. (Jul. 7, 2020), https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-52019-criteria-right-be-forgotten-search-engines_en.

198 Federico Fabbrini & Edoardo Celeste, *The Right to Be Forgotten in the Digital Age: The Challenges of Data Protection Beyond Borders*, 21 GER. L. J. 55, 60–61 (2020).

199 *Id.* at 61.

200 OECD, *Artificial Intelligence in Society*, at 104 (2019), https://doi.org/10.1787/eedfee77-en.

201 *Id.*

202 Fabbrini & Celeste, *supra* note 199, at 59, 64.

203 Yann Padova, *Is the Right to Be Forgotten a Universal, Regional, or 'Glocal' Right?,*

settlement proposal in the above case.[204] Nevertheless, the court finally denied validity of geo-blocking measures concerning RTBF application.[205]

Adversely, the territorial scope of RTBF enforcement has been broadened in a week after *Google v. CNIL* as CJEU in *Eva Glawischnig-Piesczek v. Facebook*[206] held that it was justified in applying the injunction measures for deleting offensive online content and the access blocking for such content in EU member states, but whether and how to implement them practically rested with the national rules.[207] However, there are still many issues and conflicts if the delisting and access-restricting measures are taken worldwide.[208] In short, not only the Art 17 GDPR itself cannot provide cohesive guidance for the search engines to delist URLs effectively, but also the case law of CJEU does not clarify the process of enforcing RTBF regarding *inter alia*, the geographic scope of the right, which derogates from its effectiveness.[209]

Additionally, the anonymization,[210] pseudonymization[211] and encryption approaches for RTBF application may all have disadvantages.[212] In other words, when using these measures, the data controller could encounter application problems including *inter alia*, the rejection by the court (if the measure has not been recognized by the case law)[213] and the quite decryption of the data for security and surveillance reasons.[214] Even worse, based on GDPR itself, these novel means do not seem to be consonant with the language in Article 17 (1) as this provision explicitly asks for the "erasure".[215] Therefore, the new measures which locate outside the word projection of "erasure or forgotten" in GDPR and the case law could be problematic.[216]

---

9 INT'L DATA PRIV. L. 15, 26–27 (2019).

204 *Id.* at 18.

205 Google v. CNIL, Case C-507/17, ECLI:EU:C:2019:772, ¶ 32 (Sept. 24, 2019).

206 Eva Glawischnig-Piesczek v. Facebook, Case C-18/18, ECR 1-821 (2019).

207 *See* Fabbrini, *supra* note 199, at 62.

208 *See id*.

209 *See id*.

210 ML and WW v. Germany App (Ger. V Ger,), Judgement, 2018 I. C. J. 3, ¶ 12 (June 28).

211 *See* Villaronga et al., *supra* note 13, at 310.

212 *See* Politou et al., *supra* note 95, at 1251.

213 ML and WW v Germany App (Ger. V Ger,), Judgement, 2018 I. C. J. 30, ¶ 105 (June 28).

214 *See* Olivia Gonzalez, *Cracks in the Armor: Legal Approaches to Encryption*, 2019 UNIV. ILL. J. L. TECH. & POL'Y 1, 9 (2019).

215 European Parliament Commission General Data Protection Regulation 95/46, art. 17(1), 2016 O.J. (EC).

216 These alternative measures also include deletion by default, expiration dates, down-ranking, unlearning of algorithms etc., which are not "foreseen" in the GDPR. *See* HELENA U. VRABEC, DATA SUBJECT RIGHTS UNDER THE GDPR, 150 (2021).

3. Enhanced Value Debate: Forgetting and Remembering

The responsibilities' distribution uncertainty makes RTBF ineffective in accommodating the ML environment. This partly attributes to the fierce dispute over the values behind this right.[217] In the digital age, the common perception, scope, and lawful basis of privacy rights always change once new technologies emerge.[218] Consequently, the value debate seems to be escalated in the ML context. [219] The debating values are for and against "forgetting", the former of which stands for privacy or personal dignity[220] and the latter of which indicates economic efficiency, public access to information, journalistic interests and freedom of speech.[221]

There are criticisms of the judgment of *Google Spain* about the feasibility and the adequacy of the de-linking performance.[222] This polemic is strengthened in the ML context as many scholars, on the one hand, are aware of the impracticability of striking all the data and information that is socially and economically valuable out of the systems.[223] Instead, they find that the data is easy to retain.[224] The critics also argue that as digital technology continues to be labeled "creepy," the expectation of privacy can naturally be degraded.[225] On the other hand, advocates for data protection opine that personal data deserves increasing protection because the unpredictable and uncontrolled algorithmic data processing can cause more severe damage to individuals than traditional privacy infringement.[226] Thus, the inherent value balance in RTBF needs to be

---

217 *See* Kamrul Faisal, *Balancing between Right to Be Forgotten and Right to Freedom of Expression in Spent Criminal Convictions*, 4 Security and Privacy 1, 2 (2021).

218 *See* Yulia Razmetaeva, *The Right to Be Forgotten in the European Perspective*, 10 TALTECH. J. EUR. STUD. 58, 62 (2020).

219 *See* Antoon De Baets, *A Historian's View on the Right to be Forgotten*, 30 INT'L. REV. L. COMPUTS. & TECH. 57, 57–8 (2016) (arguing that the right to be forgotten "carries an element of coercion...its net result is that the person exercising it diminishes, if not censors, the right to information of others...it affects the right to free expression.").

220 *See* Post, *supra* note 83, at 993.

221 *See* MEG LETA JONES, CTRL + Z: THE RIGHT TO BE FORGOTTEN 54–55 (2016).

222 Samuel W. Royston, *The Right to Be Forgotten: Comparing U.S. and European Approaches*, 48 ST. MARY'S L.J. 253, 260–61 (2016) (arguing that the analysis of *Google Spain* gave "too much power to the individual" and offered "insufficient credit to the basic fundamental rights of others, including the freedom of expression and the right to information.").

223 Joanna Kessler, *Data Protection in the Wake of the GDPR: California's Solution for Protecting "the World's Most Valuable Resource,"* 93 S. CAL. L. REV. 99, 100 (2019).

224 Esposito, *supra* note 119, at 5.

225 Omar Tene & Jules Polonetsky, *A Theory of Creepy: Technology, Privacy, and Shifting Social Norms*, 16 YALE J.L. & TECH. 59, 73 (2013) (arguing that as "technological innovation accelerates, so does the need to recalibrate individual expectations," and "social norms").

226 *See* Wachter, *supra* note 43, at 497–98 (arguing that AI methods "can be used to

readjusted in line with the ML features.[227]

However, the current RTBF stipulation is unlikely to harmonize the two contrasting arguments effectively.[228] Article 17 GDPR prescribes the standards for applying RTBF on the below conditions: (1) unnecessary for collection and processing purposes; (2) withdrawal of the previous consent or no other legal grounds to retain; (3) individual objection to processing data; (4) illegal data processing; (5) legal compliance in EU laws or state laws and (6) unapproved collection of the sensitive children's data.[229] Also, the RTBF requests and subsequent litigations should compromise with some justified interests in Article 17,[230] including the freedom of expression and information, legal obligations realizing the public interests or granted by authorities, allowable processing of specific categories of data, and special activities such as scientific or historical research.[231] The GDPR also requires the data controllers to delete or delist certain information within a month of receiving the request.[232]

These stipulations favor the protection of the users' information privacy rather than the right to access information in the interest of content publishers.[233] This is because controllers are demanded to take down the information expeditiously, which precipitates reckless decisions without meticulously weighing and balancing all the interests and lacks justified procedures to hear from both sides fairly.[234] This imbalance could be aggravated in the machinery context where the online platforms as information stewards or trustees need to tackle more complex scenarios created by the unpredictable and naturally discriminated algorithms and to make a decision in a short period of time.[235] Consequently, evaluating the interests is problematic.[236] From the technical perspective, once the information is erased instantly, serious destruction will be engendered in ML

---

nudge or manipulate us, or to make important decisions...about us.").

227 *Id.* at 551–54.

228 *See id.* at 551 (stating that "the GDPR does not prescribe a specific balance between data subjects' right to erasure and the legitimate interest of controllers).

229 Martha Garcia-Murillo & Ian MacInnes, *Così fan tutte: A Better Approach Than the Right to be Forgotten*, 42 TELECOMM. POL'Y. 227, 228 (2018); European Parliament Commission General Data Protection Regulation, art. 17(1), 2016 O.J. (L 119) 43, 44.

230 Post, *supra* note 83, at 987.

231 European Parliament Commission General Data Protection Regulation, art. 17(3), 2016 O.J. (L 119) 44.

232 European Parliament Commission General Data Protection Regulation, art. 12(3), 2016 O.J. (L 119) 40.

233 Dawn Carla Nunziato, *The Fourth Year of Forgetting: The Troubling Expansion of the Right to Be Forgotten*, 39 UNIV. PA. J. INT'L. L. 1011, 1055–56 (2018) (arguing that GDPR's terms "will create an unprecedented imbalance in the Internet ecosystem in favor of data subjects' erasure requests and against the right to access and right to publish information").

234 *Id.* at 1056–58.

235 *See* Wachter, *supra* note 43, at 497; Peguera, *supra* note 71, at 486–87, 501–02.

236 *See* Peguera, *supra* note 71, at 486–87, 501–02.

agents as data flows are seen as the "new oil" for the digital economy.[237]

Additionally, in the ML era, the concepts of the contradictory values behind RTBF will be necessary to be reframed and the balance of them to be readjusted. On the one hand, personal data protection needs to be understood in a more subtle and technical manner because our social connections can be transformed into digitalized datasets but this is always not a perfect transformation due to the unpredictability of the machines, possibly resulting in, for instance, an incomplete profile of an individual.[238] Hence, the lost and incomputable elements of digital profile need to be found and well protected. This means that the personal data should be selectively and specifically collected and processed under the full knowledge of the computing and social background to avoid "totalitarianism of bits."[239] On the other hand, the arguments against RTBF are displayed in various forms coexisting with the ML nature.[240] For instance, making each online speech could drive the collection and processing of a large number of datasets, provoking the risks of mass surveillance and manipulation and thus damaging the freedom of speech.[241] Also, the definition of speech needs re-consideration as the auto-generated algorithmic products are likely to be recognized as speech.[242]

Other justifications against RTBF, such as access to information and economic growth, tend to be more prominent than before.[243] Firstly, ML mediums are data-driven, consuming myriads of datasets to become operative and innovative.[244] As a result, enterprises are striving for maximizing the collection of information to grasp market advantages along with renewing their ML systems and these actions explicitly demonstrate the economic value of the data and information.[245] Secondly, the advancement of ML continues to demand

---

237 *See* Jack M Balkin, *Free Speech in the Algorithmic Society: Big Data, Private Governance, and New School Speech Regulation*, 51 U.C. DAVIS L. REV. 1149, 1155 (2018).

238 *See* Mireille Hildebrandt, *Privacy as Protection of the Incomputable Self: From Agnostic to Agonistic Machine Learning*, 20 THEORETICAL INQUIRIES IN L. 83, 91–92 (2019).

239 *Id.* at 96.

240 *See* Balkin, *supra* note 238, at 1153, 1155.

241 *See id.*

242 *See* Stuart Minor Benjamin, *Algorithms and Speech*, 161 UNIV. PA. L. REV. 1445, 1446–1447 (2013).

243 The machines are deployed in the "digital commercial and policy environment" which is more necessary to be focused on than data privacy. *See* Talia B. Gillis & Josh Simons, *Explanation < Justification: GDPR and the Perils of Privacy*, 71 J. L. & INNOVATION 71, 74 (2019).

244 *See* Bertin Martens, *The Importance of Data Access Regimes for Artificial Intelligence and Machine Learning* 5 (JRC Digital Economy Working Paper 2018-09).

245 *See id.*

open access or data transparency to the public based on social value of ML[246] and to prevent the legal and compliance challenges of the unexpected results derived by AI.[247] This may cause problems such as the leakage of personal information when the data controllers are explaining the process of ML to the public.[248] However, the RTBF stipulations in GDPR appear to be unable to address this new value debate as Article 17(3) does not take the transparency and economic benefits into consideration of the exceptions of RTBF.[249] The integrity of the ML system may be destroyed if the data has been withdrawn and the issue of destruction is outside the purview of the law application.[250] Above all, the conflict between privacy protection and other countering justifications for disentitling RTBF on the ML basis is likely to be more serious and has no relation to GDPR itself.[251]

III. POTENTIAL SOLUTIONS

Researchers and Institutions have made suggestions for adapting RTBF to the ML landscape from various perspectives, including redesigning the law in light of the cyberspace regulation theories and exploring the new technical tools to realize RTBF.[252] However, it is better to consider interdisciplinary solutions involving the interplay between human reviews and automated systems to deal with RTBF issues as the single movement of either technology or law cannot get the best effect.[253] The data controllers, especially the large online intermediary platforms such as Google and Facebook which process data through their own ML agents, are decisive in implementing the interdisciplinary solutions because they are information gatekeepers and their activities can immensely affect the democratic and fair data usage.[254] Therefore, the crux of solving the above issues

---

246 *See* Rustad, *supra* note 97, at 373.

247 *See* Jim Shook, Robyn Smith & Alex Antonio, *Transparency and Fairness in Machine Learning Applications*, 4 TEX. A&M J. PROP. L. 443, 451 (2018).

248 As the norm "transparency" requires a communicative, complicated and contextualized information disclosure, data controllers may tell data subjects extra information including other's personal information to satisfy the requirement. *See* Heike Felzmann et al., *Transparency You Can Trust: Transparency Requirements for Artificial Intelligence between Legal Norms and Contextual Concerns*, 6 BIG DATA & SOC'Y 1, 7–8 (2019).

249 European Parliament Commission General Data Protection Regulation 2016/976, art. 17, 2016 O.J. (L119) 1, 31 (EU).

250 *See* Matthew Humerick, *Taking AI Personally: How the E.U. Must Learn to Balance the Interests of Personal Data Privacy & Artificial Intelligence*, (2018) 34 SANTA CLARA HIGH TECH. L.J. 393, 408.

251 *See* Rustad, *supra* note 97, at 372.

252 *See* Kwik, *supra* note 89, at 58–64.

253 *See* JONES, *supra* note 222.

254 Mariarosaria Taddeo, *The Civic Role of OSPs in Mature Information Societies, in*

is how the digital giants develop measures combining legal and technological elements to exercise RTBF in light of the cyberspace regulation theories.

A. The Theme of Cyberspace Regulation

Cyberspace regulation theories are suitable to address the above issues as according to them, the platform intermediaries play a key role as a connecting point between individual online actors in exercising innovative tools of RTBF.[255] These theories concentrate on the nuanced, dynamic but coordinated cyberspace regulation landscape shaped by the interplay between human and non-human actors.[256] The computer codes and their writers, likely to be mediums or members of the intermediary platforms, control and dominate the entire landscape.[257]

The network communitarianism theory contends that cyberspace is a complex humanoid society and the connections and information flow amongst the actors should be simplified in the core of the Internet system by skimming and filtering.[258] The regulatory model of this theory is proactive and dynamic, requiring the regulators to ex-ante design the regulatory framework to the effect that a particular information flowing from the general cyber community to the individuals and small communities needs to be comprehensively censored and screened by the intermediaries in a democratic way representing the common interests.[259] Because the online intermediaries exert significant influence on the information control among cyber-communities, regardless of the information flow being interrupted or constantly kept, the intermediaries bear a burden of creating or designing always updated regulatory measures to optimize the fair and reasonable actions of information, consequently generating numerous responsibilities. [260]

Furthermore, there has been a newer theory called the ANT-Foucauldian Power Lens, which underlines intermediary power in network systems and focuses on the formation of this power together with its assorted and miscellaneous effects.[261] Based on this theory, the power is shaped by the human

---

OXFORD HANDBOOK OF ONLINE INTERMEDIARY LIABILITY, 11 (Giancarlo Frosio ed., 2020).

255 *See* Kwik, *supra* note 89, at 62.

256 *See id.* at 63.

257 LAWRENCE LESSIG, CODE AND OTHER LAWS OF CYBERSPACE LAWS: VERSION 2.0, 124–25 (2nd ed., 2006).

258 *See* ANDREW MURRAY, INFORMATION TECHNOLOGY LAW: THE LAW & SOCIETY, 200–01 (4th ed. 2019).

259 *Id.* at 201.

260 *Id.*

261 *See* Vranaki, *supra* note 15 at 172.

or non-human actors affected by interactive material or intangible legal, social and technological contents, denoting a sense of the synthesis of legal, social or market effects.[262] Vranaki, one of the theory's advocates, states that Facebook is likely to establish a routine of authentic consent based on the mutual interaction between social, legal, and technological actors.[263] Also, RTBF as a GDPR right can be configured within the algorithmic systems of online intermediaries based on the communications of diverse actors, similar to the form of valid consent envisaged by Vranaki.[264] This means that the application of RTBF should be expanded and renewed in order to render the intermediaries adaptable to this dynamic and heterogeneous regulatory framework.[265]

While some criticize that network communitarianism tends to create an imbalance inclined to human actors instead of non-human actors[266] and to define the regulatory framework as a global and societal scheme, overlooking the contributions of individual and independent elements,[267] these theories, if put together, will be attractive based on the above reasoning. Therefore, it seems that the essence of cyberspace regulation theories lies in the online intermediaries by organizing technical, legal, and other aspects of solutions to undertake managing and operational responsibilities of RTBF application in the ML context.[268]

B. Technical Solutions

To fulfill the aim of RTBF application in the ML context in line with the above theories, there have been diverse technical solutions brought out by scholars for the online service providers, with social and legal, active and passive factors combined.[269] Some researchers have worked out new technical tools for the machines to "forget" data effectively, including "the decremental update ML procedures" presented by Schelter,[270] the ubiquitous encryption mechanism

---

262 *Id.* at 6–7.

263 *Id.* at 33–34.

264 *Id.* at 33.

265 For example, the UK is considering to change its digital regulation and data protection framework to reduce the unnecessary burden on the data controllers. It criticizes the inflexible compliance regime which GDPR prescribes and suggest a proactive, systematic, and flexible platform accountability with "the governance, policies, tools, people and skills" combined for data protection. *See* UK Department for Digital Culture Media & Sport, Data: A New Direction, (10 September 2021), p. 53, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1022315/Data_Reform_Consultation_Document__Accessible_.pdf.

266 Vranaki, *supra* note 15 at 172.

267 Kwik, *supra* note 89, at 61.

268 *See id.* at 62.

269 *See* HELENA U. VRABEC, DATA SUBJECT RIGHTS UNDER THE GDPR, 151–52 (2021).

270 SEBASTIAN SCHELTER. NEW YORK UNIVERSITY, "AMNESIA"- TOWARDS MACHINE

driven by algorithmic computing which enables the data subjects to decrypt their personal data only by using special passwords,[271] and the effective deletion algorithms designed by Ginart et al.[272] However, these tools are only efficient and reliable in the literary works, without being examined in practice, similar to the comment of Villaronga et al. on anonymization, pseudonymization and encryption methods.[273] The authors turn to believe that data deletion is not the ultimate target of the RTBF technologies but stratified standards of technical solutions should be embraced.[274] This not only requires new tools for the forgetting process, but also for collecting and archiving stages, which can increase the effectiveness of the RTBF.[275] Again, the authors recognize that multidisciplinary or multidimensional solutions including legal and social concerns should be taken seriously rather than focusing on the mere technical part.[276]

In addition, Esposito re-explains the meaning of "forgetting the digital memory", which is diluting the link between the algorithmic index and the accurate data source by adding many disturbing and false contents to "confuse" the algorithmic processing instead of removing or encrypting the identifiable data.[277] This approach is called "forgetting without remembering."[278] In this way, the effectiveness deterioration of the algorithms and the problem of impossible exhausted "forgetting" mentioned above can be eschewed, but this measure still produces the equivalent result as deletion and de-identification.[279] Overall, doubtlessly, as the ML technology will become increasingly popular and prevail in the future, the technical sphere of establishing connections between the ML environment and RTBF or other important individual data rights will also blossom and be diversified.[280] In other words, if the technical solutions assimilate into the legal and social backgrounds, the full picture of RTBF application will be brighter.

LEARNING MODELS THAT CAN FORGET USER DATA VERY FAST, 1 (2019).

271 Orin S. Kerr & Bruce Schneier, *Encryption Workarounds*, 106 GEO. L.J. 1, 3 (2018).

272 *See* ANTONIO A. GINART ET AL., Stanford University, MAKING AI FORGET YOU: DATA DELETION IN MACHINE LEARNING, 1 (2019).

273 Villaronga et al., *supra* note 13, at 310.

274 *Id.* at 305.

275 *Id.* at 311.

276 *Id.*

277 Esposito, *supra* note 119, at 6.

278 *Id.*

279 *Id.* at 7.

280 Jim Shook, Robyn Smith & Alex Antonio, *Transparency and Fairness in Machine Learning Application*s, 4 TEX. A&M J. PROP. L. 443, 444–45 (2018).

C. Legislative Approaches

The GDPR has been criticized for its failure to create a legal framework conditioned on lawfulness, impartialness and transparency of ML although efforts have been made to cope with this issue.[281] For instance, applicable stipulations for automated data processing may become ineffective when confronted with inherently non-transparent datasets or dynamic data flows for various and indiscernible processing purposes.[282] This legislative problem of RTBF still exists as the specific data and its processing purposes should be identified for further forgetting steps.[283] As a result, it is suggested that algorithmic technologies themselves can automatically distinguish if the above grounds are enough for data processing under the current legal framework without human intervention.[284]

In contrast, other scholars argue that how the data will be used should be explained and is subject to a connotative right named "the Right to Explanation" in the GDPR.[285] This right enables the data subjects to request "the meaningful information about the logic involved" of the algorithmic processing from the data controller and processor pursuant to Art. 13(2)(f), 14(2)(g) and 15(1)(h) GDPR.[286] Article 22(3) further asks for safeguards for the data subject after he/she has received the explanation, including human intervention of the subject on the controller's side to comment on and challenge the algorithmic decision, which has legal effects on the subject if the data processing is mainly automated.[287] Accordingly, no matter if data subject's intervention appears, it is online intermediaries (namely data controllers/processors as Google defined in *Google Spain*) that should carry legal duties to reveal the ML process by configuring basic settings of its algorithms to make them transparent and justified in line with the right to explanation, which requires providing meaningful information to data subjects.[288] This is also true in the case of RTBF, as the request receivers and deletion/de-indexing operators are data controllers/processors who possess algorithmic mediums and are accountable

---

281 *See* Christopher Kuner et al., *Machine Learning with Personal Data: Is Data Protection Law Smart Enough to Meet the Challenge?*, 7 INT'L DATA PRIV. L. 1, 2 (2017).

282 *Id.* at 1–2.

283 European Parliament Commission General Data Protection Regulation 679, art. 17, 2016 O.J. (L 119) 1.

284 *See* Kuner et al., *supra* note 282.

285 *See* Andrew D Selbst & Julia Powles, *Meaningful Information and the Right to Explanation*, 7 INT'L. DATA PRIV. L. 233, 233–34 (2017).

286 *Id.*

287 *Id.* at 235.

288 *See* Margot E Kaminski & Gianclaudio Malgieri, *Algorithmic Impact Assessments under the GDPR: Producing Multi-layered Explanations*, 11 INT'L DATA PRIV. L. 125, 144 (2021); Sec. 2(7) and Sec. 3, H.R.6580 - Algorithmic Accountability Act of 2022, 117th Congress (2021–2022).

for creating a fair, socially significant and transparent functioning environment of ML.[289] The lawmakers should therefore recognize the expected ML landscape and precisely design the accountabilities for the intermediaries to test and adopt new forgetting projects, which consequently necessitates a more nuanced interpretation of GDPR.[290]

D. The Intermediary Responsibility

Summarizing the above analyses from different perspectives, the idea of combining the technical, legislative, and social elements (which is presented in the legislative and technical solutions) and focusing on online intermediaries is the point to realize RTBF in the ML layout. The first challenge remarked earlier is how to keep the "forgetting" requests of data subjects valid while the importance of the right to information and freedom of expression is emphasized simultaneously. The GDPR apparently sets an example in this respect, which asks online platforms to impose a temporary ban on access to the data in dispute when the data subject has sent a removal request.[291] At the moment, the online intermediaries are hesitating about the ultimate deletion, delisting or other technical operations.[292] Keller nonetheless claims that interest-balancing actions can be taken only if other legislations such as the eCommerce Directive could be interpreted to include the "notice and immediately take down" process within the RTBF application.[293] Meanwhile, the ultimate burden to enforce RTBF on those online intermediaries should be lightened.[294] This means that if the platforms have bona fide reasons to refuse data deletion, they should not be severely panelized by regulators.[295] Although this may narrow the scope of RTBF in terms of privacy or data protection, the obligations, and operations to materialize data privacy rights can be reallocated to other individual GDPR provisions if flexibly interpreted,[296] potentially mitigating the conflict between the opposing objectives. For example, the data minimization of collecting personal data stipulated in GDPR seems to be effective in protecting data privacy as the provision relieves the burden of implementing RTBF because if less data

---

289 Michael Butterworth, *The ICO and Artificial Intelligence: The Role of Fairness in the GDPR Framework*, 34 COMPUT. L. & SEC. REV. 1, 2 (2018).

290 *See* Unal Tatar et al., *Law Versus Technology: Blockchain, GDPR, and Tough Tradeoffs*, 38 Comput. L. & Sec. Rev., forthcoming, 7 (2020).

291 Daphne Keller, *The Right Tools: Europe's Intermediary Liability Laws and the EU 2016 General Data Protection Regulation*, 33 BERKLEY TECH L. J. 287, 362 (2018).

292 *Id.*

293 *Id.* at 361–62.

294 *Id.* at 362–63.

295 *Id.*

296 *Id.* at 334.

is collected, less information will be forgotten.[297] Admittedly, instead of a simple notification of data minimization, the formation of relative processes and guidelines for data controllers to collect limited data is more essential for the enforcement of the rule.[298]

Secondly, the intermediaries play a pivotal role in addressing the issue of cutting off extraterritorial access to information as *Google v. CNIL* exhibited.[299] In this case, the court suggested effective measures to be developed by search engines to "seriously discourage" users in other EU member states from accessing the disputed URLs,[300] but was unable to detail the effectiveness and the appropriate measures.[301] Hence, the liability to work out effective technical means to establish an extraterritorial de-referencing or delisting mechanism falls on the search engines, as GDPR expresses its worldwide application though being criticized as "data imperialism".[302] In fact, search engines have broadly used the geo-blocking tool to preclude access to foreign websites displaying the contents to be forgotten in the domestic networks, which is likely to be a typical example for all responsible intermediaries whereas the use of proxies or virtual private networks can bypass the block.[303] This means that it is up to online intermediaries such as search engines to adopt measures to realize the extraterritorial forgetting as the EU law aims for. [304] The intermediaries can also integrate the cross-jurisdictional duties of the prevention of data dissemination (RBTF is the EU version) as they operate internationally.[305]

More broadly, as some countries such as the U.S. at the federal level do not take the RTBF as a lawful data privacy right (while some states have it adopted),[306] it is the duty of online intermediaries to bridge the gap between the paternalistic EU laws and other national or regional legislations where personal information has not been systematically protected.[307] This is because, from the perspective of data protection authorities, it is hard to ease the ingrained

---

297 Villaronga et al., *supra* note 13, at 313.

298 *Id*.

299 Case C-507/17, Google v. CNIL, ECLI:EU:C:2019:772, ¶ ¶ 4, 54–55 (Sept. 24, 2019).

300 *Id*. ¶ 70.

301 *Id*. ¶ 71.

302 *Id*. ¶ 72–73; Jure Globocnik, *The Right to Be Forgotten is Taking Shape: CJEU Judgments in GC and Others (C-136/17) and Google v CNIL (C-507/17)*, 69(4) GRUR INT'L. 380, 386–87 (2020).

303 Google v. CNIL, ECLI:EU:C:2019:772, ¶ 43; Globocnik, *supra* note 303, at 381, 385.

304 Google v. CNIL, ECLI:EU:C:2019:772, ¶ 70.

305 *See* David Erdos, *The 'Right to be Forgotten' Beyond the EU: An Analysis of Wider G20 Regulatory Action and Potential Next Steps*, 13 J. OF MEDIA L. 1, 3 (2021).

306 Rustad, *supra* note 97, at 379.

307 *Id*. at 376.

conceptual conflict between data privacy protection[308] and opposing values including freedom of expression.[309] This conflict is explicitly illustrated and increasingly exacerbated by the failure of the safe harbor agreement between U.S. and EU.[310]

However, non-legislative measures suggested by Rustad and Kulevska equip themselves with the social, market, and technical means to bypass the conflicting legislative standards of RTBF application in various legal systems, while the measures preserve the merits of the grounds against the right.[311] These measures should be adopted by network intermediaries as they are the knots connecting to different network matrixes given by the network communitarian theory.[312] For example, Google once carried out a program enabling an individual, who was mentioned in a specific online content referenced by Google News, to verify his/her relationship to the information by adding comments below, making readers understand why the specific information should not be forgotten.[313] This seems to be a successful attempt to realize RTBF without changing the laws,[314] but only by technical adjustments in online intermediaries. These actions get rid of the unclear definition of the "effective forgetting" in GDPR to some extent.

Thirdly, to disentangle the uncertain standard of "forgetting" in ML systems, the mere amendment of GDPR is deficient in this regard, as the law is always behind technological development.[315] However, in the EU, the law urges online intermediaries to act proactively in terms of data protection and thus imposes numerous liabilities thereon.[316] It means that the online platforms could become "secondary lawmakers," who take the responsibility of converting the fixed policy texts into a dynamic and adaptive self-regulatory mechanism.[317] This is approved at the theoretical, ethical, and moral level as the intermediaries can be

---

308 Steven C. Bennett, *The Right to be Forgotten: Reconciling EU and US Perspectives*, 30 BERKELEY J. INT'L. L. 161, 168–69 (2012).

309 ANDREW MURRAY, INFORMATION TECHNOLOGY LAW: THE LAW & SOCIETY, 92–93 (Oxford Univ. Press, 4th ed. 2019).

310 Yann Padova, *The Safe Harbour Is Invalid: What Tools Remain for Data Transfers and What Comes Next?*, 6 INT'L DATA PRIV. L. 139, 139–40 (2016).

311 Rustad, *supra* note 97, at 386.

312 CHRIS REED & ANDREW MURRAY, RETHINKING THE JURISPRUDENCE OF CYBERSPACE, 159–60 (2018).

313 Rustad, *supra* note 97, at 385.

314 *Id.* at 384.

315 Villaronga et al., *supra* note 13, at 312.

316 Hiroshi Miyashita, *The "Right to be Forgotten" and Search Engine Liability* 12–13, (Brussels Priv. Hub Working Paper No. 8, 2016), https://brusselsprivacyhub.eu/BPH-Working-Paper-VOL2-N8.pdf.

317 Giancarlo F. Frosio, *Why Keep a Dog and Bark Yourself? From Intermediary Liability to Responsibility*, 26 INT'L. J.L. & INFO. TECH. 1, 13 (2018).

seen as a proxy supporting the public interests in online society.[318] Also, the EU Commission is eager to forward online private enforcement to form a regulatory mechanism at the heels of technological development, notwithstanding the negative effects of arbitrary decisions and unclear distributions of responsibilities.[319] In the context of RTBF application within ML agents, despite decentralized trend of law/policy application and enforcement, the online intermediaries can independently determine the best way to forget the digital memories, at their discretion according to the intermediary responsibility.[320]

Apart from the legal-binding options such as deletion and delisting, there are self-deployed measures available including the "proactive monitoring" and "algorithmic implementation."[321] These self-mandated approaches could be useful for efficiently enforcing RTBF, as the imperceptible marks of data to be forgotten are more likely to be revealed under continuous surveillance.[322] In addition, Peter Fleischer puts forward the "three degrees of deletion", stratifying the scope of data to be deleted and the online intermediaries can take this into consideration when they are designing the "forgetting tools" but unsure of the breadth of effects of the tools.[323] Accordingly, online intermediaries bear the primary responsibility to apply laws, social norms and updating technologies to make RTBF more applicable in the ML environment.[324]

IV. CONCLUSION

RTBF has been recognized as a fundamental right for data subjects in the digital era and it has taken dozens of years for RTBF to be settled down in statutory language of data protection law since its initial forms, the right to oblivion, as well as the right to erasure, was created.[325] This right nevertheless encounters loads of issues about the application in its interplay with advanced ML technology.[326] This article has described primary technological elements of ML to draw a whole functioning picture of the technology. The elements include algorithms, large clusters of datasets and the neuron network as the base to run algorithms.[327] It seems that the text of RTBF is perceptively unrelated to these elemental technologies of ML, but the application of RTBF will inevitably

---

318 *Id.* at 15.
319 *Id.* at 13–14.
320 *Id.* at 32–33.
321 *See id.* at 20.
322 *See id.* at 21.
323 Rustad, *supra* note 97, at 387–89.
324 Daphne Keller, *The Right Tools: Europe's Intermediary Liability Laws and the EU 2016 General Data Protection Regulation*, 33 BERKLEY TECH. L. J. 287, 296–97 (2018).
325 *See* discussion *supra* Sections 2.2.1 and 2.2.2.
326 *See supra* Part 3.
327 *See supra* Part 1.

involve them.[328] This could raise problems both pertinent to the damage of the sound ML mechanism and the validity of the RTBF itself.[329] Unfortunately, GDPR fails to recognize this problem and thus a change needs to be set about.

It is claimed that the issues are not merely caused by the drawbacks of the law and the whole situation is not solely influenced by the legal factors.[330] Thus, an all-round view of these problems is essential, which can trace to the technical, legal, and even social roots of the law.[331] Firstly, from the legal perspective, the lack of a cohesive definition of the term "forget" and the confusion of the benchmark to enforce this right under GDPR, quasi-legislative guidelines and case law can lead to the inapplicability of this right.[332] Also, in some special scenarios, the absence of matching legal obligations and responsibilities of crucial organizational cyberspace participants to the RTBF enforcement results in the application failure.[333] Secondly, from the technical viewpoint, in light of the optional approaches to realize RTBF summed up by the laws, either these approaches are infeasible in the ML context, or the performance of ML agents will be diminished.[334] Lastly, under the social or theoretical background, the controversy between social or personal values pros and against RTBF proceeds to be intensified in the ML ecosystem.[335] Respectively, the legal and technical measures should be adjusted based on the latest outcome of the debate.

The solutions suggested in this article have referred to the popular cyberspace regulation theories, some of which propose a multifaceted network regulation with law, technology and social norms instilled.[336] These theories believe that online intermediaries play an important role in forming the solutions to "forget" digital memories in the ML environment.[337] The online intermediaries should also adopt these solutions through the interconnections with other actors participating in the RTBF application or ML process, which underline the responsibility of stewardship for those intermediaries. Hence, this article has specified the technical and legal measures and concluded with the proactive intermediary responsibilities of information management and control.

---

328 *See supra* text accompanying notes 117–122.
329 *See supra* text accompanying notes 120–122.
330 *See supra* Section 3.2.
331 *See supra* text accompanying notes 151–157.
332 *See supra* Section 3.1.
333 *See* discussion *supra* Section 3.1.2.
334 *See* discussion *supra* Sections 3.2.1 and 3.2.2.
335 *See* discussion *supra* Section 3.2.3.
336 *See supra* notes 266–275 and accompanying text.
337 *See supra* Section 4.1.