International Research Journal on Advanced Engineering and Management
https://goldncloudpublications.com
https://doi.org/10.47392/IRJAEM.2024.514
e ISSN: 2584-2854
Volume: 02
Issue:12 December 2024
Page No: 3479-3488

Ethical Imperatives and Technical Realities: Implementing the Right to be Forgotten in Artificial Intelligence

Sriram G[1], J. Junita Sarah[2], J.B. Rupa Vahini[3]
[1,2,3]Student, Saveetha School of Law, SIMATS, India.
Email ID: *smartsriram21@gmail.com[1], junitalaw.2006@gmail.com[2], rupavahinijb2005@gmail.com[3]*

Abstract
The "Right to be Forgotten" (RTBF) has become a crucial aspect of data privacy in the digital age. It addresses the challenges of managing and erasing personal data in a world dominated by artificial intelligence (AI) and machine learning (ML). This paper examines the implementation of RTBF within AI and ML systems. It includes a comparative analysis of regulatory frameworks in the European Union (EU), the United States (US), and India. The EU's General Data Protection Regulation (GDPR) sets a global benchmark with explicit provisions for data erasure and RTBF. It requires AI systems to comply with strict data handling and deletion protocols. In contrast, the US lacks a federal RTBF regulation, relying instead on a patchwork of state laws and sector-specific regulations. This presents unique challenges and opportunities for AI and ML practitioners. India's Digital Personal Data Protection Act (DPDP) introduces RTBF focusing on consent and transparency, aiming to balance innovation with privacy concerns. This paper explores the technical and legal implications of implementing RTBF in AI and ML, including data minimization, retraining models, and the ethical considerations of balancing individual rights with the collective benefits of data-driven technologies. The implementation of RTBF should also be carefully handled alongside other legal rights such as the right to freedom of speech and expression. By examining case studies and current practices, this research offers insights into developing robust RTBF mechanisms that align with diverse regulatory landscapes, ensuring that AI and ML advancements are achieved without compromising fundamental privacy rights.

Keywords: *Right to be Forgotten, Artificial Intelligence, Regulation, Personal Data, Technologies*

1. Introduction

As the world strives to become more efficient and effective day by day, it uses all possible means to achieve its goal, which includes technology. Technological developments have taken a stronghold in the coming days and are seen to be infiltrating every aspect of life, A few examples of sophisticated innovations are blockchain, quantum computing, machine learning, and artificial intelligence. This increasing area of technology also means an increasing need for regulating the same, and various countries are fronting in that too, including the European Union, South Korea, and India. In this paper, we will be discussing one such aspect of regulation: digital rights with special reference to the Right to Be Forgotten in the context of Artificial Intelligence in both European and Indian environments. European Union has been a leading actor in this race as they have implemented regulations and there is an increasing ruling regarding the same. It's crucial to address this research area because people lack awareness regarding the potential use of their data by big tech companies. The increasing risk of data misuse poses a threat of irreparable harm to individuals' lives. It can be seen as evidence in many social media platforms where data that is updated on the internet becomes a digital footprint that can never be erased, which cannot be an accepted norm because it's data relating to a person, and that data cannot be taken for granted and kept on a public domain for an indefinite period if the data subject has not consented for the same. This poses a significant threat to one's autonomy or in more legal

International Research Journal on Advanced Engineering and Management
https://goldncloudpublications.com
https://doi.org/10.47392/IRJAEM.2024.514
e ISSN: 2584-2854
Volume: 02
Issue:12 December 2024
Page No: 3479-3488

form, one's self-determination over his or her data, though it is a prevalent notion that "internet never forgets", it can't be accepted when it can hurt one's life on a personal level [1-4].

1.1. Research Objectives

1. To define the Right to be forgotten and its significance.
2. To explain the existing regulations concerning RTBF in the European Union and India.
3. To explain the scope and challenges in the application of RTBF in AI models.
4. To discuss the possible solutions for law-abiding AI models.

2. Literature Review

CHENG-CHI CHANG has navigated through emerging challenges in the implementation of the RTBF in an AI model and has explored the feasibility of the same per the GDPR stipulations. He has highlighted the challenges such as privacy, data protection, and the feasibility of forgetting. The ultimate finding that he has arrived at is that the RTBF should be established as a separate right instead of confining them to be a part of the privacy and reputational rights. the authors have advocated for recognizing the technical and legal challenges in implementing RTBF in AI and have advocated for creating a regulatory framework to overcome the same, which will ensure that technological innovation is not hindered in safeguarding individual rights and vice versa. BUSRA BILSIN: The thesis intends to investigate the application of the Right to Be Forgotten (RTBF) in text creators and its interaction with the General Data Protection Regulation (GDPR). It examines how text creators collect and handle personal information and the difficulties in meeting GDPR obligations, particularly in terms of data deletion. The document also discusses the intricacies of balancing RTBF with freedom of speech and proposes technological and policy resolutions to encourage the proper implementation of the RTBF within the GDPR framework. In addition, discussions are also on the scope and extent of RTBF in the given AI models. Finally, the paper discusses the feasible technical remedies and policy suggestions that are supposed to be in place for the compliance of the text producers in accordance with the GDPR framework. The study has also acknowledged the limited scope of the feasible options, conclusively, the thesis has underscored the need for a realistic approach to realizing data erasure in an AI environment. JESUS L. Lobo, Sergio Gil-Lopez, And Javier Del Ser: The document addresses the difficulties of implementing the Right to Be Forgotten (RTBF) in AI systems, particularly in light of varying privacy laws across different countries. The authors emphasize the intricacies involved in removing personal data from AI models and suggest several areas of AI research that could aid in addressing RTBF, such as machine unlearning, generative modelling, federated learning, and transfer learning. The authors advocate for further exploration of AI models that honour RTBF, particularly in contexts involving sensitive data, as a comprehensive solution to the RTBF challenge in AI is still not fully developed. Tiffany Li, Eduard Fosch Villaronga, Peter Kieseberg: The article addresses the concept of the Right to be Forgotten concerning privacy laws. It stresses the importance of closer collaboration between legal and technical aspects to tackle the difficulties in implementing and enforcing legal requirements in data-processing systems. It also underscores the disparity between human memory and artificial intelligence capabilities. It concludes by highlighting the essential nature of interdisciplinary research in confronting the challenges presented by artificial intelligence and in harmonizing legal frameworks with rapidly advancing technologies. Dawn Zhang and others delve into the intricacies of integrating the right to erasure within large language models (LLMs). The right to erasure allows individuals to request the removal of their data, but its enforcement in LLMs is complicated due to the interconnected and extensive nature of training data. The paper outlines technical, legal, ethical, and operational hurdles, such as the challenge of identifying and deleting specific data and the need to strike a balance between privacy and freedom of expression. The proposed remedies include differential privacy, federated learning, and enhanced data tagging and indexing. The authors provide case studies and experiments to illustrate the feasibility of

International Research Journal on Advanced Engineering and Management
https://goldncloudpublications.com
https://doi.org/10.47392/IRJAEM.2024.514
e ISSN: 2584-2854
Volume: 02
Issue:12 December 2024
Page No: 3479-3488

these solutions, emphasizing the trade-offs between model performance and enforcing the right to erasure. The paper concludes that effectively addressing the right to erasure in LLMs necessitates a multidisciplinary approach and continuous collaboration among researchers, policymakers, and industry stakeholders to devise practical and efficient solutions [5-9].

3. Research Methodology

This research paper adopts a doctrinal legal research methodology, which involves a systematic and detailed analysis of legal texts and materials. Doctrinal research is traditionally focused on the examination of primary legal sources such as statutes, case law, and regulations, as well as secondary sources including legal commentaries, textbooks, and journal articles. Through this method, the study aims to interpret and analyse the existing legal framework, understand its development, and propose potential reforms or new interpretations to address identified gaps or inconsistencies. By critically evaluating legal principles and judicial decisions, this research seeks to provide a comprehensive understanding of the current state of the law and suggest some guidelines to be followed for the day to come [10-15].

4. Research Problem

The idea of the "Right to be Forgotten" (RTBF) in digital privacy is increasingly recognized. While it has been seen successfully implemented in traditional internet space, the same is a significant challenge in AI-driven models. Existing literature often focuses on regulatory frameworks and lacks empirical studies on practical integration strategies for RTBF in AI and ML. The absence of consistent global standards further complicates matters. It is commendable to see initiatives taken by various players such as the EU and India. On the Europe front, it is the General Data Protection Regulation (GDPR) and Digital Personal Data Protection Act (DPDP) in India. Both the regulations are welcoming, as they prioritize consent and transparency in obtaining and processing personal data, but realizing these in the real world is not an easy task at hand. The list of challenges is endless such as practical barriers, examining diverse regulatory environments, balancing the interests of various stakeholders concerning the data, and so on. Addressing these gaps involves navigating technical hurdles and ethical considerations at the intersection of technology and law, as the problem at hand is a by-product complex mix of various disciplines.

4.1. Research Questions

1. What is the Right to be Forgotten (RTBF) in the context of the Artificial Intelligence (AI) and Machine Learning (ML) era?
   a) Right to be Forgotten.
   b) Significance of RTBF in the digital age.
   c) Approach of RTBF in traditional internet and AI model.
2. What are the regulatory frameworks to implement RTBF in AI and ML models?
   a) European Union
   b) India
   c) United States
3. What are the scope and challenges of implementation of RTBF in AI and ML?
4. What are the possible solutions for the implementation of RTBF?
5. What is the Right to be Forgotten (RTBF) in the context of the Artificial Intelligence (AI) and Machine Learning (ML) era?

a) The Right to be Forgotten is a person's right to remove their unwarranted or incorrect information from the public domain to prevent misuse of such information which may result in significant damage to their reputation and possible damage to their day-to-day life. The same information can be also removed from the database for other valid reasons such as the expiry of the time or purpose for which the data was provided, etc. The RTBF was first recognized officially by the Court of Justice of the European Union (CJEU) in the case of Google Spain.2 This concept first originated from French Jurisprudence in the concept of the “Right to Oblivion” and various other countries including India recognized and implemented these rights in a quasi-form such as anonymity. RTBF is not just a right on the ambit of Digital Privacy rights but also falls within the ambit of both Fundamental Rights under the right to privacy and Human rights.

b) Significance of RTBF in the digital age: Privacy

International Research Journal on Advanced Engineering and Management
https://goldncloudpublications.com
https://doi.org/10.47392/IRJAEM.2024.514
e ISSN: 2584-2854
Volume: 02
Issue:12 December 2024
Page No: 3479-3488

is one the fundamental elements of Human Rights and securing the same in the digital age will ensure that no form of excuse can be used to descent anyone from protecting their rights. Tech companies have understood the value of individual data, and they collect and process a vast amount of data for personalizing their service to their target customers. In this space, we as consumers are not very aware of the rights related to our personal data in a digital space, and this might result in the loss of self-determination over our data. This amplified the need for legislators to act, which is not limited to a few provisions empowering each one of us with RTBF. The Internet also has developed significantly from just mail and search engines to machine learning and LLM-based AI models. LLM-based AI is an algorithm capable of generating entirely original content, such as text, images, or code, using the information they were provided during training. Developments in this area, particularly with the emergence of large language models (LLMs) such as ChatGPT, have sparked increased fascination with generative AI. This is done by training them on large data and although their performance sounds optimal, their capacity to remember and recall information brings up substantial worries about the concept of the right to be forgotten.

c) Approach of RTBF in traditional internet and AI model: The right to be forgotten is a digital privacy right that can be enforced by removing personal data from the internet by removing that website from the online domain in the form of de-listing, etc. But the same concept cannot be applied when it comes to AI and ML models as they are learning algorithms that have processed the Big Data (means a huge volume of data) into their training framework and have developed into Large Language Models (LLM) which produce text, we can simply call it a “text producer”. So, for a comprehensive understanding of the existing limitations in applying the same method of implementing RTBF, we need to understand the working phenomenon of each model, in the traditional internet model, for example: a search engine, which searches the information from wide internet sources and provides reasonable relevant information, but on contrary the AI models have already processed the huge amount of data before deployment, so they are not obligated to go in search of any online source rather it produces its output with the memory that has developed during their training framework [16-19].

6. What are the regulatory frameworks to implement RTBF in AI and ML models?
   a) The European Union (EU) was not just a pioneer in recognizing and implementing RTBF, but also in imbibing the same in their regulatory framework which is the General Data Protection Regulation (GDPR),8 but it’s pertinent to note that this is a successor of the EU Directives of 1995.9 But this concept evolved through a series of cases, where the RTBF took a dominant position over the other conflicting rights. Legal Grounds (European Union):1.Right to be informed: Every data subject(users) has the right to be informed about if, when, and why their data is being collected, and if the data of the data subject is being collected from other sources, it must be informed within one month. 2.Right of Access: Individuals have the right to access information regarding the processing of their data, it includes all forms of information such as if, when, how, how long, purpose, etc. The right also includes the right to be aware of processing details and to decide whether such action is necessary and based on the convenience of the data subject, we can choose to invoke other rights. 3.Right to Rectification: The data subjects are empowered to rectify any inaccurate information from the controller. 4.Right to erasure: The data subject has the right to remove any of their data from the data controller, and this can be exercised in cases where the data are inaccurate, unconsented, etc.14 The same right is also not absolute and

International Research Journal on Advanced Engineering and Management
https://goldncloudpublications.com
https://doi.org/10.47392/IRJAEM.2024.514
e ISSN: 2584-2854
Volume: 02
Issue:12 December 2024
Page No: 3479-3488

can be denied on certain grounds.15

b) India still has not yet explicitly recognized the RTBF as a legal right, but it was noted as an integral part of the Right to Privacy in the famous judgment16, but the Indian \courts have not taken any proactive steps regarding the same, but the same right is enforceable in digital space as per the Digital Personal Data Protection Act (DPDP) of 202317 which enables the data subjects to remove or edit any unconsented personal data or incorrect data from the public domain.

c) Legal Grounds (India): The Digital Personal Data Protection Act provides the right to erasure under section 12 of the act, and such right allows the data principal(user) to rectify, remove, and update any of their data from the data fiduciary. The same act also provides certain grounds to process the data for given legitimate purposes as mentioned in Section 7 of the act, which are: for the purpose for which the data was provided by the data principal,19, etc. The Act includes provisions to empower the state to process the data under any law that time is in force and also in cases of emergency, disaster, etc. Neither Europe nor India considers the Right to Erasure to be an absolute right and the same can be denied in certain cases, which is also very similar. But in the case of Europe, the right is well recognized, whereas in the case of India, it is still in the budding stage though it has legal backing.

d) The United States (US) does not have any federal law to substantiate the RTBF, but they do have various laws limiting it to its use within the state.20 The US courts have created a stronghold for Freedom of speech and expression rights over any privacy-related right; to worsen it, the US has not even recognized the Right to Privacy as a fundamental right due to its constitutional framework which upholds the right to freedom of speech and expression over privacy.

7. What is the scope of implementation of RTBF in AI models?

a) The implementation of RTBF concepts has a lot of existing challenges in AI models, which was already discussed above in describing the working phenomenon of AI model and traditional internet model. As we are clear with the existing technical issue on a nascent level, now we will dwell on the same in a detailed manner further in the paper. Even the above-discussed regulation also mandates AI models to implement RTBF, but the feasibility of the same is debatable with the existing technological advancements.

4.2. Scope and Challenges in Implementing RTBF

The Right to be Forgotten can be extended and applied in any public domain including search engines, AI models, Machine Learning algorithms, etc. The implementation of RTBF in the AI model has ambiguity at its preliminary stage itself, though the GDPR (we will be using this as a default regulation) enforces the RTBF concept, it not only advocates for restricting access to the data but for complete elimination of data from the database. But while dwelling on the technical feasibility of the same, we might conclude that with given technical advancement it is only possible to restrict the accessibility of the data, which can be substantiated by the below-mentioned challenges. These challenges cannot be isolated in their nature, so the challenges that will be discussed will be multifaceted including both technical, legal, and notional [20-25].

4.2.1. Duplication of Data & Territorial Jurisdiction

Subjecting information that is made public by the original publisher is an easy task at hand as it can be made possible to make the original publisher take down that information, but when data gets duplicated and posted on other websites or platforms cause challenges, so in this situation, restricting the access to the data becomes a feasible option. And even the original data that can be regulated comes under question when we discuss territorial jurisdiction. As we all know the internet is spread across borders, and so is the data on the internet. To highlight this

International Research Journal on Advanced Engineering and Management
https://goldncloudpublications.com
https://doi.org/10.47392/IRJAEM.2024.514
e ISSN: 2584-2854
Volume: 02
Issue:12 December 2024
Page No: 3479-3488

concern, we can refer to the case of CNIL (French Data Protection Authority), where the CNIL fined Google for not delisting data from all domains including the ones outside the EU, but the same undermines the regulatory sovereignty of others, so it would be reasonable to establish geo-blocking technology, the same was also done by Google but this move will be futile when the data can be accessed with the help of VPN technology. This becomes a major concern since various countries have a stark contrast of approach, for example: the EU considers the Right to privacy, and RTBF is within the four walls of fundamental and human rights. On the contrary, the US gives more priority to freedom of speech and expression and does not even consider the Right to privacy as a fundamental right and the same is the case in various countries.

4.2.2. Difference in Working Phenomenon of AI Model and Traditional

Internet: Let us discuss this again in a deeper understanding of the challenges in the context of AI. One of the most prominent and preliminary challenges we face is our inability to treat both traditional internet and AI models as the same because the output that is produced by an AI model is from the inbuilt data or memory that is developed by the model during their training period, but whereas the output produced by the search engine is by surfing through a vast web data that is available externally. This reason the well-formulated output produced by a text producer compared to a search engine, but when we talk about removing the data from a text producer, we are talking about the model with numerous neural links and a complex training framework, where a huge amount of data is scraped from the internet and various other sources, for instance, AI like DALL-E, and GPT-4 are trained on a diverse and massive amount of data that spans over billions of parameters and endless interconnection of neural networks within in model and also includes the various patterns of learning. This endless process of acquiring data is also known as “Data Hunting”.The AI that is trained in such a manner develops strong memory and inherently loses the ability to ‘forget’, as they are designed to use all available data for optimized output.29 How we are going to locate the data and delete the same has not yet been answered conclusively to consider it as an option30 and this also proposes other ideas such as re-training the model and other options to delete data without actually retraining the entire model but none of which can be implemented without affecting the output of the AI models.

Data Hallucination: It is a concept where the synthetic output that is provided by the AI models is factually incorrect, but this flaw made by the AI cannot be attributed to the presence of inaccurate or inadequate data in the dataset that these models are trained on, rather it is a byproduct of models design and its ability to produce their original content creatively, this includes LLM producing inaccurate citations and wrong conclusion from the context, though various companies train to model with various counter-hallucination technology and strategy, it is an inevitable problem.

Transparency: It is an attributing factor to most of the challenges we face in implementing RTBF in AI, the lack of transparency on the working of the AI model complicates the job of addressing various challenges. There is a declining trend of transparency in LLM as can be evidenced in OpenAI and Meta AI's move to protect the details of GPT-4’s architecture and Llama 2 training datasets. As per the Stanford Foundation Model Transparency Index qualifies GPT-4 to be 48% and Llama 2 to be 54% transparent. If this trend is allowed to continue, it will reduce our chance of identifying and rectifying or removing data embedded within the complex AI algorithm.

4.2.3. Balancing the Interests of Various Stakeholders

Discussing the data that is available in the public domain has various focuses of interest attached to it and allows us to discuss the legal grounds of the RTBF. The GDPR provides the following rights for individuals: The right to be informed; access; rectification; erasure; restrict processing; data portability; object; and rights concerning automated decision-making and profiling34 these are rights that pertain only to individuals, but also there are other rights of other stakeholders such as the right to be informed and the right to freedom of speech and expression in the interest of the public at large and the

International Research Journal on Advanced Engineering and Management
https://goldncloudpublications.com
https://doi.org/10.47392/IRJAEM.2024.514
e ISSN: 2584-2854
Volume: 02
Issue:12 December 2024
Page No: 3479-3488

data processors. Balancing these rights in a particular situation is a complex task and creates a question of authority because for every instance court cannot be approached, in this case, the appropriate solution can be the establishment of an internal committee or department within the organization and also in all cases it cannot be said to have balancing these rights in their decision. There are stipulated provisions in both GDPR (EU context) and DPDP (Indian context), where they have established exemptions and grounds for invoking RTBF, but the chance of misinterpretation is high in implementation, credit for the same can attributed to the broad and vague nature of rights involved.

4.3. What are the Possible Solutions for the Implementation of RTBF?

Before we dwell on the possible solutions to implementing RTBF in the current context, it is necessary to understand, what is the definition of personal data, so we can understand why and how far the below suggested solution is effective. As per GDPR, Article (1) defines the criteria for data to be regarded as personal data, which is "any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person". As we can see, it is quite an expansive definition and includes both direct and indirect means. Where Indian context, The DPDP, defines it to be "means any data about an individual who is identifiable by or in relation to such data" and it defines data to be "means a representation of information, facts, concepts, opinions or instructions in a manner suitable for communication, interpretation or processing by human beings or by automated means". As we are now, we are aware of what is data and what is personal data in both European and Indian contexts, and we will move forward. Time and again we have discussed that at the contemporary level, there are no compelling solutions to implement RTBF in an algorithm environment such as AI and ML implemented at the industry practice level, there are few developments in this area of research, such as :Machine Unlearning is of two types exact and approximate machine unlearning, in the Exact Machine Unlearning method, we develop a new model to be trained from scratch by removing the deleted data to ensure no impact on the performance of the model35, but while doing this, we need to change the entire algorithm framework which renders it to be a more challenging process. Approximate Machine Unlearning is a concept where the data is removed from the model without actually retraining the model from scratch, but the complex and unpredictable working of the model hinders the understanding of how solitary data location can be traced and altered in the complex web neural link, but this paradigm application has various other limitations such as the relevance of the data in the model may be unknown due to the complicated nature of training and removing data from the model lower the quality of output, compared to the output that it produced pre-unlearning stage. It cannot also be conclusively stated whether the data is actually forgotten by the trained model. Though this application has its limitations, it can be considered to be a better way of implementing RTBF as per GDPR guidance rather than merely making data inaccessible, which was done in the Google Spain case. Generative Learning refers to the model using the Generative Adversarial Networks or the modern Stable Diffusion Models, where the model undergoes training through a limited amount of data and anonymous data, this reduces the possibility of the model being affected by RTBF applications. But this also does not negate the possibility of invoking RTBF applications. Federated Learning and Transfer Learning is an approach where there is a limit to the addition of model parameters by keeping the majority of parameters fixed, this significantly reduces the computation and storage requirements, this is one of the approaches to mitigate the chance of RTBF. The federated unlearning algorithm was proven to be efficient and effective in unlearning data by Liu, Xu, Yuan, Wang, and Li in medium-scale public datasets, opening a greater potential for building data deleting FL services in various applications. Privacy-

International Research Journal on Advanced Engineering and Management
https://goldncloudpublications.com
https://doi.org/10.47392/IRJAEM.2024.514
e ISSN: 2584-2854
Volume: 02
Issue:12 December 2024
Page No: 3479-3488

preserving Machine Learning (PPML) is a method of training where the model will be adhering to various concerns about privacy threats by making the model go through multiple phases in countering privacy threat actions such as Private Data in the Clear, Model Inversion Attacks, Membership Inference attack, De-anonymisation, and Reconstruction Attack. One of the aspects of PPML is Differential Privacy (DP), (source) demonstrated that the model with DP can perform without losing its efficiency in producing synthetic data and the data that is produced by the model can used again by the model for their further training. Again, the synthetic data that is used to train the data is a very small portion of data that is fed into the model, so this cannot ensure complete protection of privacy. Privacy by design: A common way of looking at AI adhering to RTBF is in the stage of post-development, it is better to reverse-engineer the approach and try to design a model that can comply with the stipulated regulations. The proposed model will adhere to all privacy concerns and regulations not by command but rather by default design, the same is also hinted in GDPR, which includes measures such as data minimization, encryption, pseudonymization, and anonymization. Anonymization is the most compelling method, as the GDPR stipulates personal information to be information that can be attributed to a person, once data gets anonymized by the model during training or before training, the data falls short of fulfilling the essentials to invoke RTBF, the same has to be done is a way that eliminates the feasibility of finding the same data in alternate ways, but that can't be promised and has the risk of potential re-identification. To counter these challenges in the anonymization method, the concept of randomization techniques emerges, where the association between the data and the data subject is manipulated by introducing randomness to avoid the implication of RTBF, but this method is also in the developing stage. In this design, almost every stage of training of the model should have a privacy and transparency check, but this design is an ideal notion and not yet a feasible real-world practice.

5. Discussion on Solution

Protecting the RTBF in all forms in the AI era: There should be an increase in the area of focus on regulating AI, the trajectory of AI being non-profit shifting more towards a capitalistic approach which increases the chance of prioritizing profit over safety, and also the same market leaders deploy their LLM models labeled as "research preview" or "experiment", but this seems nowhere to be falling closer to definition of scientific research. This has to be brought to the eyes of the regulators and has to be addressed. Tailored legal protection: It should be provided for diverse right-holders instead of using a blanket approach, it will ensure a more human approach is taken and it is always better to have regulations based on the needs of the stakeholders which will ensure that we do not negate special care to those in need, such as minors, mentally ill individuals, public figures or officials, criminals, etc. Self-Regulation: One of the most feasible methods to regulate is by allowing the self- regulation concept which can ensure the development of robust methods in regulations. The same can be seen as evidence in proactive measures taken by the tech industry in adapting OECS's AI principles, this depicts the potential of responsible use of AI and Self-regulation. To cement this approach, we can discuss Meta's Oversight Board, which allows content modification on a uniform legal system, but we must also be careful not to allow this autonomy-yielding power of the tech companies to be focused only on corporate goals rather than public interest. International framework: As we have discussed above, it is necessary to have an international framework to be established for the harmonious application of the law, it equally important to respect the territorial jurisdiction and sovereignty of each country while we invoke RTBF in the interest of the individual's right, this will also help us in avoiding any unwanted clash of interest between countries. Harmonious approach techno-legal approach: It is vital to find an equilibrium point in balancing both technical and legal solutions to this issue because we cannot restrict the interest of AI innovation for the sake of individual privacy and vice versa. For a start, we can rely on the blueprint provided under the "Ten Principles for Regulation That Does Not Harm AI Innovation" by the Information Technology and

International Research Journal on Advanced Engineering and Management
https://goldncloudpublications.com
https://doi.org/10.47392/IRJAEM.2024.514
e ISSN: 2584-2854
Volume: 02
Issue:12 December 2024
Page No: 3479-3488

Innovation Foundation. It addresses the issues of tailored regulation and consists of other guidelines balancing both law and technology for adapting future breakthroughs. Transparency: It is imperative to put forth the necessary measures to improve the transparency in the processing of data to ensure that it is on legitimate legal grounds and to provide the data subject with the necessary ways to exercise their rights to rectify or remove inaccurate data. Transparency and accountability are paramount in gaining public trust and this aspect also ensures self-regulations are done fairly and transparently. Algorithm Governing Committee: An Autonomous Algorithm Committee would ensure the compliance of tech companies to the regulatory standards of the industry, and this will ensure effective supervision of risk management throughout the data lifecycle, handling data deletion rejections, algorithm-based corporate disputes, etc. On this front, Italy's data protection authority "Italian Garante" and French data protection authority "CNIL" initiatives stand as ideal examples.

Conclusion

Digital privacy concerns are an inevitable challenge in an increasingly digitalized world, it is imperative for us to research and develop solutions to the digital threats that we face now and, in days to come. As we have discussed some solutions above, they are not an exhaustive list of studies or research on this area, there are more areas such as the question of whether synthetic data of a trained model could be considered to be personal data, Does the right to erasure contain a right to full retraining of an ML model? etc. So, there is an endless list of considerations in this very specific area of RTBF in the context of AI alone. In the Indian context, there are significant developments in regulations including the advisory issued by the Ministry of Electronics and Information Technology. But more to be done to secure privacy on the AI model, taking more steps on this front will ensure that the privacy rights of the future generation are not breached in the excuse of innovative technology. "Start by doing what's necessary; then do what's possible; and suddenly you are doing the impossible."- St Francis of Assisi. A quote to remember, we started by doing what was necessary and possible, and it's time we do the impossible and achieve justice for those in need.

References

[1]. Google Spain SL, Google Inc. v Agencia Española de Protección de Datos, Mario Costeja González (2014)
[2]. (2018) Privacy law: Right to be forgotten in India I. Available at: https://nliulawreview.nliu.ac.in/wp-content/uploads/2022/01/Volume-VII-17-33.pdf (Accessed: 22 July 2024).
[3]. Bilsin, B. (2023) Navigating EU Data Protection Law: The Challenge of the Right to Be Forgotten in AI- Driven Text Producers. thesis.
[4]. Friedland, A. (2024) OpenAI vs. NYT - the copyright fight and the future of AI training, AI in the FY2024 NDAA, and two Gao reports on ai, Center for Security and Emerging Technology. Available at: https://cset.georgetown.edu/newsletter/january-18-2024/ (Accessed: 22 July 2024).
[5]. Chang, C. (Kirin) (2024) 'When AI remembers too much: Reinventing the right to be forgotten for the generative age', SSRN Electronic Journal [Preprint]. doi:10.2139/ssrn.4868555.
[6]. GDPR
[7]. EU DIRECTIVE 1995
[8]. Google Spain SL, Google Inc. v Agencia Española de Protección de Datos, Mario Costeja González, (2014)
[9]. Zhang, D. et al. (2024) Right to be Forgotten in the Era of Large Language Models: Implications, Challenges, and Solutions. thesis.
[10]. Justice K.S. Puttaswamy & Anr. vs. Union of India & Ors, (2017)
[11]. DPDP 2023
[12]. Section 12 of the DPDP act
[13]. Subclause a of section 7 of DPDP Act.
[14]. Bettelhäuser, P.F. (2022) AI & the Right to be Forgotten under the GDPR. thesis.
[15]. Chang, C. (Kirin) (2024) 'When AI remembers too much: Reinventing the right to be forgotten for the generative age', SSRN

International Research Journal on Advanced Engineering and Management
https://goldncloudpublications.com
https://doi.org/10.47392/IRJAEM.2024.514
e ISSN: 2584-2854
Volume: 02
Issue:12 December 2024
Page No: 3479-3488

Electronic Journal [Preprint]. doi:10.2139/ssrn.4868555.
[16]. Miller, K. (2023) Introducing The Foundation Model Transparency Index. rep.
[17]. Zhang, D., Pan, S., et al. (2024) 'To be forgotten or to be fair: Unveiling fairness implications of machine unlearning methods', AI and Ethics, 4(1), pp. 83–93. doi:10.1007/s43681-023-00398-y.
[18]. Lobo, J.L., Lopez, S.G. and Ser, J.D. (2023) The right to be forgotten in artificial intelligence: Issues, approaches, limitations and challenges | IEEE conference publication | IEEE Xplore. Available at: https://ieeexplore.ieee.org/document/10195023 (Accessed: 22 July 2024).
[19]. Hu, H. et al. (2024) Network and distributed system security (NDSS) Symposium, NDSS Symposium. Available at: https://www.ndss-symposium.org/ (Accessed: 22 July 2024).
[20]. Liu, Y. et al. (2022) 'The right to be forgotten in federated learning: An efficient realization with rapid retraining', IEEE INFOCOM 2022 - IEEE Conference on Computer Communications [Preprint]. doi:10.1109/infocom48880.2022.9796721.
[21]. Juliussen, B.A., Rui, J.P. and Johansen, D. (2023) 'Algorithms that forget: Machine unlearning and the right to erasure', Computer Law & Security Review, 51, p. 105885. doi: 10.1016/j.clsr.2023.105885.
[22]. Big Data, artificial intelligence, Machine Learning and ... Available at: https://ico.org.uk/media/for-organisations/documents/2013559/big-data-ai-ml-and-data-protection.pdf (Accessed: 22 July 2024).
[23]. Castro, D. (2023) Ten Principles for Regulation That Does Not Harm AI Innovation. rep.
[24]. Google LLC v the Commission Nationale ne l'informatique et des Libertés
[25]. Revised AI advisory: How ai regulation can impact India (2024) INDIAai. Available at: https://indiaai.gov.in/article/revised-ai-advisory-how-ai-regulation-can-impact-india (Accessed: 22 July 2024).