INTERNATIONAL JOURNAL FOR LEGAL RESEARCH AND ANALYSIS

Open Access, Refereed JournalMulti Disciplinary
Peer Reviewed Edition :

www.ijlra.com

 ISSN: 2582-6433

DISCLAIMER

ISSN: 2582-6433

EDITORIAL TEAM

EDITORS

Megha Middha

Megha Middha, Assistant Professor of Law in Mody University of Science and Technology, Lakshmangarh, Sikar

Megha Middha, is working as an Assistant Professor of Law in Mody University of Science and Technology, Lakshmangarh, Sikar (Rajasthan). She has an experience in the teaching of almost 3 years. She has completed her graduation in BBA LL.B (H) from Amity University, Rajasthan (Gold Medalist) and did her post-graduation (LL.M in Business Laws) from NLSIU, Bengaluru. Currently, she is enrolled in a Ph.D. course in the Department of Law at Mohanlal Sukhadia University, Udaipur (Rajasthan). She wishes to excel in academics and research and contribute as much as she can to society. Through her interactions with the students, she tries to inculcate a sense of deep thinking power in her students and enlighten and guide them to the fact how they can bring a change to the society

Dr. Samrat Datta

Dr. Samrat Datta Seedling School of Law and Governance, Jaipur National University, Jaipur. Dr. Samrat Datta is currently associated with Seedling School of Law and Governance, Jaipur National University, Jaipur. Dr. Datta has completed his graduation i.e., B.A.LL.B. from Law College Dehradun, Hemvati Nandan Bahuguna Garhwal University, Srinagar, Uttarakhand. He is an alumnus of KIIT University, Bhubaneswar where he pursued his post-graduation (LL.M.) in Criminal Law and subsequently completed his Ph.D. in Police Law and Information Technology from the Pacific Academy of Higher Education and Research University, Udaipur in 2020. His area of interest and research is Criminal and Police Law. Dr. Datta has a teaching experience of 7 years in various law schools across North India and has held administrative positions like Academic Coordinator, Centre Superintendent for Examinations, Deputy Controller of Examinations, Member of the Proctorial Board

ISSN: 2582-6433

Dr. Namita Jain

Head & Associate Professor

School of Law, JECRC University, Jaipur Ph.D. (Commercial Law) LL.M., UGC -NET Post Graduation Diploma in Taxation law and Practice, Bachelor of Commerce.

Teaching Experience: 12 years, AWARDS AND RECOGNITION of Dr. Namita Jain are - ICF Global Excellence Award 2020 in the category of educationalist by I Can Foundation, India.India Women Empowerment Award in the category of "Emerging Excellence in Academics by Prime Time & Utkrisht Bharat Foundation, New Delhi.(2020). Conferred in FL Book of Top 21 Record Holders in the category of education by Fashion Lifestyle Magazine, New Delhi. (2020).Certificate of Appreciation for organizing and managing the Professional Development Training Program on IPR in Collaboration with Trade Innovations Services, Jaipur on March 14th, 2019

Mrs.S.Kalpana

Assistant professor of Law

Mrs.S.Kalpana, presently Assistant professor of Law, VelTech Rangarajan Dr. Sagunthala R & D Institute of Science and Technology, Avadi.Formerly Assistant professor of Law,Vels University in the year 2019 to 2020, Worked as Guest Faculty, Chennai Dr.Ambedkar Law College, Pudupakkam. Published one book. Published 8Articles in various reputed Law Journals. Conducted 1Moot court competition and participated in nearly 80 National and International seminars and webinars conducted on various subjects of Law. Did ML in Criminal Law and Criminal Justice Administration.10 paper presentations in various National and International seminars. Attended more than 10 FDP programs. Ph.D. in Law pursuing.

Avinash Kumar

Avinash Kumar has completed his Ph.D. in International Investment Law from the Dept. of Law & Governance, Central University of South Bihar. His research work is on "International Investment Agreement and State's right to regulate Foreign Investment." He qualified UGC-NET and has been selected for the prestigious ICSSR Doctoral Fellowship.He is an alumnus of the Faculty of Law, University of Delhi. Formerly he has been elected as Students Union President of Law Centre-1, University of Delhi.Moreover, he completed his LL.M. from the University of Delhi (2014-16), dissertation on "Cross-border Merger & Acquisition"; LL.B. from the University of Delhi (2011-14), and B.A. (Hons.) from Maharaja Agrasen College, University of Delhi. He has also obtained P.G. Diploma in IPR from the Indian Society of International Law, New Delhi.He has qualified UGC – NET examination and has been awarded ICSSR – Doctoral Fellowship. He has published six-plus articles and presented 9 plus papers in national and international seminars/conferences. He participated in several workshops on research methodology and teaching and learning.

ISSN: 2582-6433

ABOUT US

INTERNATIONAL JOURNAL FOR LEGAL RESEARCH & ANLAYSIS ISSN

2582-6433 is an Online Journal is Monthly, Peer Review, Academic Journal, Published online, that seeks to provide an interactive platform for the publication of Short Articles, Long Articles, Book Review, Case Comments, Research Papers, Essay in the field of Law & Multidisciplinary issue. Our aim is to upgrade the level of interaction and discourse about contemporary issues of law. We are eager to become a highly cited academic publication, through quality contributions from students, academics, professionals from the industry, the bar and the bench. INTERNATIONAL JOURNAL FOR LEGAL RESEARCH & ANALYSIS ISSN 2582-6433 welcomes contributions from all legal branches, as long as the work is original, unpublished and is in consonance with the submission guidelines.

ISSN: 2582-6433

THE GDPR'S RIGHTS-BASED APPROACH TO AI DEVELOPMENT

AUTHORED BY - ABEER SHRIVASTAVA

The importance of data to the development of AI applications is a well-known fact. Since the previous decade, when the industry began to focus on the application of machine learning to process vast volumes of data, artificial intelligence has made tremendous progress. In machine learning systems, data correlations are discovered, and corresponding models are constructed, which logically tie multiple 'possible inputs' to 'potentially correct replies.' In machine learning applications, after being trained and educated on many examples, artificial intelligence systems learn to make predictions. As a result, artificial intelligence has become increasingly 'hungry' for data, and this need has fuelled data collection, creating a self-perpetuating vicious cycle: the development of AI systems based on machine learning requires and promotes the creationof massive data sets, also known as big data. The combination of artificial intelligence with massive amounts of data has the potential to deliver significant benefits for economic, scientific, and societal progress. However, it also contributes to people's and society's worries,such as extensive surveillance and its influence on citizen behaviour, polarisation and fragmentation in the public realm, etc. Many applications utilising artificial intelligence manage personal information. A personal data set can be utilised to train machine learning systems and, consequently, develop their algorithmic models. Personal information can also beadded to data sets used to train machine learning systems. Such models can be applied to personal data to derive inferences about particular individuals. As a result of artificial intelligence, all forms of personal data can be utilised to analyse, predict, and affect human behaviour, providing a valuable chance to transform such data and their processing results intovaluable commodities. In domains such as healthcare, for instance, where complicated decisions must be made based on a variety of circumstances and undefined criteria, artificial intelligence enables automated decision-making. Artificial intelligence systems can avoid typical psychological errors and be subjected to stringent restrictions, making automated forecasts and conclusions not only more cost-effective, but also more accurate and impartial inmany cases than human ones. In contrast, algorithmic conclusions may be erroneous or biased,mimicking human biases while introducing new ones. Even when automated assessments of individuals are fair and accurate, they have flaws: they

ISSN: 2582-6433

may have a negative impact on the participants, who are subjected to pervasive observation, constant review, constant influence, and even manipulation. (Sartor 2020). It provides the door to new kinds of social knowledge and improved governance, but also raises the prospect of 'surveillance capitalism' and 'surveillance state' as extremes. (Sartor 2020)

In addition to government regulation and public enforcement, the countervailing power of civil society is required to discover abuses, inform the public, and mobilise enforcement in order to adequately safeguard citizens from the threats posed by artificial intelligence misuse. Citizen empowerment technology based on artificial intelligence, for instance, might play a key role in this respect by enabling citizens to detect illegal practises, identify instances of unjust treatment, and distinguish between phoney and unreliable information, among other things. (Sartor 2020)

Relationship with GDPR

The General Data Protection Regulation and artificial intelligence are neither friends nor foes. In certain instances, the General Data Protection Regulation (GDPR) restricts or, at the very least, complicates the processing of personal data within an AI environment. However, if we continue to progress toward a fully regulated data market, it may eventually aid in establishing the trust necessary for consumers and government officials to accept artificial intelligence. The General Data Protection Regulation and artificial intelligence will always exist mutually. As more artificial intelligence and data-specific legislation emerge throughout Europe and the world, we can expect their relationship to mature and solidify. (Spyridaki 2020)

Prior to the GDPR, the EU's highest court, the European Court of Justice (ECJ), gave broad interpretations of data privacy regulations in cases where personal data was being processed or put at risk due to a lengthy and complex process. The European Court of Justice heard a case on October 19, 2016, in which the German government was accused of violating the right to privacy by recording dynamic IP addresses. (*Breyer v Deutschland, 2016 C-582/14*) Accordingto the ECJ, certain IP addresses are protected under the DPD because controllers can "likely reasonably" correlate their data with that of a third-party system that contains personally identifiable information to identify specific users. The European Court of Justice displayed a liberal interpretation of data protection regulations when it ruled that ostensibly anonymous information can be used to identify a person if it is potentially exploited by a third party. This expansive holding occurred under the less comprehensive DPD, so it is reasonable to anticipate

ISSN: 2582-6433

that a presumption of infraction will almost certainly exist under the more restricted but broadly defined GDPR. (Humerick 2006)

The purpose of the GDPR is to simplify data processing by establishing uniform data privacy and protection standards. However, according to the European Commission, the GDPR's rapid implementation, coupled with the high standards it establishes, threatens to result in enormous liability risks for data controllers and processors around the world. Based on current AI development models, machine learning and big data will cause businesses around the globe to fall under the GDPR, regardless of whether they are aware of it or not. This liability risk wouldbe significantly higher for unsupervised Al models, which by definition have little to no human control. If an organisation falls within the GDPR's scope, it must comply with its regulations, which is easier said than done. Even if a controller is located outside the European Union, Article 3 is likely to hold them liable, particularly if they wish to conduct business with EU- based firms or trade with EU-based companies. Companies found guilty face severe penalties,including "administrative fines of up to 20,000,000 EUR or, in the case of an undertaking, up to 4 percent of the previous fiscal year's total worldwide annual revenue, whichever is greater."(GDPR A. 83 (6)) Based on the repercussions alone, certain companies may be dissuaded fromdeveloping Al. Because Al's current development model does not comply with the GDPR's provisions, the following provisions threaten to impede Al's development: (1) the right to consent; (2) the right to be forgotten (erasure); (3) the right to data portability; and (4) the rightto explanation. (Humerick 2006)

Conflicts

1. *Right to Consent*

While the General Data Protection Regulation (GDPR) specifies several legal bases for the processing of personal information, the most prevalent method for lawfully processing Personally Identifiable Information (PII) of consumers is through explicit consent for one or more specific purposes. The European Union takes an opt-in approach to data privacy, meaning that controllers may only process personal information with the data subject's explicit and unambiguous consent. Article 7 places the burden on the controller to demonstrate, among other things, that the data subject consented expressly and voluntarily. When it comes to children, additional responsibilities are incurred. Under the General Data Protection Regulation, a child under the age of sixteen is prohibited from consenting, though individual Member States

ISSN: 2582-6433

may lower the age to thirteen. A controller may limit its liability by making "reasonable efforts" to verify consent, whether through the parent or the child's age; however,these efforts must take into account the available technology and the circumstances. (GDPR A.7) However, the GDPR does not define "reasonable efforts," and because available technology must be taken into account, courts may be more critical of controllers and processors as a result. Obtaining consent is a straightforward process but obtaining the right torevoke consent is a significantly more difficult challenge.

Article 7 stipulates that data subjects may withdraw their consent at any time. After consent has been withdrawn, controllers and processors may attempt to continue processing the data inother permissible ways, but such attempts risk violating the General Data Protection Regulation. Inasmuch as they have the potential to reduce the amount of data available for learning, both the requirement for consent and the ability to withdraw consent pose a threat tothe advancement of Al. In addition, data subjects have the right to request that their informationnot be processed under certain conditions. In the case of big data, for instance, a company maycollect a large amount of data for machine learning purposes only. Given that each data subjecthas consented, this Al model is lawful and unrestricted, regardless of the data collection mechanism. Consider the possibility of a data subject or group of data subjects withdrawing their consent. While the preceding processing was permissible, any future processing or disclosure of these particular data points would violate the General Data Protection Regulation (GDPR). Given that Al continues to learn from previous data, the question is how to prevent Al from learning from this input while maintaining its prior development.

This is illustrated by the current concept of deep learning based on neural networks, which depicts how Al's development is dependent on the use of a large quantity of data to continuously adapt to it’s surroundings. In theory, refusing consent and continuing learning viathe processing of previously learned behaviours would constitute a breach of the General Data Protection Regulation (GDPR). Consider the case of an Al system that learns how to respond to irate customers using tonal patterns based on accumulated data. Then, one of the data subjects requests that the controller cease processing his or her voice data. Under the GDPR, all prior learning would continue to be valid, but the Al would no longer be able to construct algorithms using these precise data references. All indications point to the Al's inability to continue learning with these data, as any subsequent learning processing would be a derivative of the original set,

ISSN: 2582-6433

which contained the withdrawn data. If the Al were to reclaim its role, it would require new data unless the processor could isolate the learning thread that had been incorporating the now-non-consensual input. Since the current Al model is based on neural networks that connect all data sources, future isolation is unlikely. The consent clause of the GDPR is anticipated to result in either widespread Al regression or ongoing liability issues forthose who continue to derive insights from unlawfully processed data. (Humerick 2006)

2. Right to be Forgotten / Right to Erasure

In addition to the right to provide and withdraw consent, Article 17 of the GDPR grants data subjects the right to have their personal information removed from the system. Article 17's "obligation" to destroy all personal data "without undue delay" is triggered by a number of events, including the revocation of consent. (GDPR A. 17) Moreover, if the data sought to be erased is in the public domain, the controller must take reasonable measures to notify other controllers that the data subject must erase the data as well as any links to it or copies of it. Because all copies of the data must be erased, a single exercise of Article 17's right to be forgotten may have a negative impact on the operations of multiple controllers.

Similar to the exercise of the right to agree, the right to be forgotten has the potential to impede Al's development. The European Commission warns that erasing personal data that is part of a larger set of big data may have a negative impact on the accuracy and dependability of the Al. For instance, when Al algorithms undergo the process of machine learning, they utilise already-available data to learn specific functions. Deleted data may result in algorithmic behaviours that differ from those observed when the data was present, rendering the algorithm less stable,less reliable, and less accurate at predicting future events. Consequently, according to some, personal information used by Al may still be considered part of the neural network even after it has been destroyed.

The fear of corporations illegally retaining personal data can be alleviated in part by requiring them to retrain their existing Al models using this updated data set. This alternative would result in the creation of Al, who would be perpetually threatened with extinction. To function properly, the Al would need to relearn what it had previously learned, which would increase research and development costs and cause delays. As a result, the Al market within the European Union would be subject to unique risks, liabilities, and costs not found on other global Al markets,

ISSN: 2582-6433

which could result in corporations ceasing operations with and within the European Union.

An alternative strategy to retraining the entire Al neural network is to develop algorithms for unlearning specific data inputs. This enables organisations to combat the issue without having to retrain the Al neural network in its entirety. This method will incur higher R&D costs and additional development time, and GDPR compliance issues may still arise. Even though the mechanics of forgetting information are unknown, businesses must develop procedures that permit the isolation and deletion of personally identifiable information (PII) from a data set. (Humerick 2006)

3. Right to Data Portability

The right to data portability enshrined in Article 20 of the European Convention on Human Rights is an additional impediment to Al expansion. Article 20 of the GDPR grants data subjects two fundamental rights: (1) the right to obtain their personal data from a controller, and (2) the right to transmit those data to another controller without delay or further processing.(GDPR A. 7) Consequently, these rights enable data subjects to contribute to the disseminationof information, potentially reducing the amount of data collection effort required by smaller data controllers. In contrast, the right to portability raises issues similar to those raised by the rights to consent and erasure.

The right to portability requires the maintenance of systems to identify and isolate a person's personally identifying information (PII). This is a simple responsibility, as is the requirement to provide the data subject with a structured report. The second right included in Article 20 may cause problems for controllers: the right to communicate data to a third party other than the controller. In addition to the ability to exercise their right to be forgotten and all the associated concerns, data subjects can now also demand that data controllers give up their competitive advantages. The acquisition of massive amounts of data is essential to Al's development under its current model; massive data sets offer a significant competitive advantage. Companies invest millions of dollars annually to improve their data collection processes. The ability to acquire or extract this information from a data subject enables smallerbusinesses to collect comparable quantities of personally identifiable data without spending asmuch money on data collection operations. It is possible that the provisions of Article 20 will result in data parity, which will ultimately lead to more competitive Al markets, which will benefit consumers. Consequently,

ISSN: 2582-6433

businesses would have a less obvious advantage or disadvantage based on the quantity of data available to them. Even though data parity may aidin the overall development of AI, it may also increase enterprise risks and have a negative impact on AI.

Businesses must prioritise public relations and data security because customers can choose who keeps their information; otherwise, data subjects may not trust controllers with their personal information. When large-scale data breaches occur, for instance, consumers' sense of being violated is immediately triggered. In this situation, consumers' lack of trust and willingness to take corrective action will almost certainly result in a demand for the transfer or deletion of their data. Thus, lavishly funded Al operations may become illegal or run out of money beforethey can continue their development. While it cannot be said that corporate espionage and sabotage will become more prevalent in the UAE, it may be contended that the potential consequences of breaches and unfavourable publicity could be catastrophic for some organisations. Lastly, consumer data portability rights are inherently fraught with the danger that a single misstep in public relations could spell the end of otherwise promising Al operations. (Humerick 2006)

4. Right to Explanation

Article 22 of the GDPR protects an individual's right not to be subject to decisions based solely on automated processing.

"Data subjects have the right to request human intervention and explanation if they do not consent to the processing." (GDPR A.22) Even though there are exceptions to this rule, processors and controllers are still required to respect the rights, freedoms, and interests of data subjects. Individuals have the right to be informed about automated decision-making, including profiling. In addition, if a data subject requests it, he or she must be provided with “meaningful information about the logic involved, as well as the significance and envisaged consequences for the data subject." (GDPR A.13)

Moreover, data subjects have the right to object to automated processing when it is carried outin the public interest or when the data subject's fundamental rights and freedoms outweigh the processing controller's or a third party's interests. In this situation, the controller must demonstrate "compelling legitimate reasons for the processing which override the data subject's interests, rights, and freedoms, or that the processing is necessary for the establishment,

ISSN: 2582-6433

exercise, or defence of legal claims." (Humerick 2006) Overall, the controller must convince the court that its personal goals outweigh the highly valued and protected data privacy rights of the people. Since the European Court of Justice (ECJ) vigorously defends consumer data privacy rights, a controller must evaluate whether the risk of GDPR violation outweighs the benefits of continuing to process the data. Even if the European Court of Justicerules in favour of the controller, a data subject may be able to restrict the processing of his or her personally identifiable information (PII) in accordance with Article 18's right to restrict processing. (Humerick 2006)

Models of unsupervised machine learning are impractical for businesses that rely on A.I. to efficiently complete tasks. Article 22 guarantees the right to human intervention and explanation of logic, necessitating that all decisions be explained. Unsupervised learning techniques, as opposed to the supervised learning model, which uses labelled data sets to construct algorithms and is supplemented by human oversight, enable Al to advance independently. Because there are no data labels or correlations between the data elements, it may be impossible to track or explain the Al's learning processes or decisions using unsupervised models. Even supervised models may be difficult to comprehend, thereby jeopardising one of Al's most valuable capabilities: the ability to make automated judgments and forecast. As a result of the GDPR's expansive protection of data privacy rights, autonomy,and automation, two of Al's most valuable characteristics, are difficult to utilise.

Although understandable, protections against individual profiling have the potential to eliminate Al's economic value and its capacity to learn. Most commercial applications of aluminium aimed at customers rely on analysis and forecasting based on the individual's uniquecharacteristics to be effective. Individuals have the right to object to processing that is used to"analyse or forecast aspects of a natural person's work performance, economic situation, health,personal preferences, interests, dependability, behaviour, location, or movements." (Humerick2006) Using limited profiling, it is not possible to learn from human, group, or individual behaviour, and it may not be viable for long-term operational applications. Under the right to object, direct marketing, which is a marketing strategy that analyses individual buyer behaviours to predict future purposes in order to tailor advertisements to specific individuals, is also clearly identified as an undesirable processing purpose. The objections to direct marketing lack a counterargument that would allow controllers to continue operations if they could provide a reasonable justification.

ISSN: 2582-6433

As a result of the GDPR, the commercial applicationof Al is constrained, which could result in companies abandoning future investments in the technology. (Humerick 2006)

Conclusion

Individuals' dignity and autonomy are compromised when they are denied the right to participate in decision-making processes that have a significant impact on their lives. In addition, it is essential to determine whether they have the authority to wield such power, as well as who is accountable for granting them such authority. Individuals and social processes could be dehumanised if we believe that automated decision making is more equitable, successful, and efficient. In addition to Article 22 paragraph 3 of the GDPR, which establishesa right to human intervention, the European Group on Ethics in Science and New Technologies Artificial Intelligence calls attention to the ongoing debate regarding the establishment of twonew rights: the right to meaningful human contact and the right not to be profiled, measured, analysed, or nudged.

In addition, autonomy and self-determination refer to the freedom of choice regarding the useof artificial intelligence, which must be voluntary and informed. It is essential to protect people's right to informational self-determination to ensure that they are always provided withrelevant information when interacting directly with an artificial intelligence system or when providing personal data to be processed by such systems. High-quality data protection and privacy protection help individuals gain confidence in the manner in which their data is processed, which encourages data exchange and, consequently, fosters workplace creativity. Solving the control problem is a prerequisite for more powerful artificial intelligence systemsto benefit society in the long run.

Bibliography

1. Sartor, Giovanni. 2020. "The impact of the General Data Protection Regulation (GDPR) on Artificial Intelligence." *Scientific Foresight Unit (STOA) Panel for the Future of Science and Technology* 100.
2. Spyridaki, Kalliopi. 2020. "SAS." *SAS Insights.* https://www.sas.com/en_in/insights/articles/data-management/gdpr-and-ai--friends--foes-or-something-in-between-.html#/.

ISSN: 2582-6433

3. Humerick, Matthew. 2006. "Taking AI Personally: How the E.U. Must Learn to Balance the Interests of Personal Data Privacy & Artificial Intelligence." *Santa Clara High Technology Law Journal* 393-418.
4. Cabral, Tiago Sérgio. 2020. "Forgetful AI: AI and the Right to Erasure under the GDPR." *European Data Protection Law Review (EDPL)* 378-389.
5. Mitrou, Lilian. 2018. "Data Protection, Artificial Intelligence and Cognitive Services: Is the General Data Protection Regulation (GDPR) 'Artificial Intelligence-Proof'?" *Available at SSRN: https://ssrn.com/abstract=3386914*.
6. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679 accessed May 8th, 2022.
7. *Breyer v Deutschland, 2016 C-582/14* https://curia.europa.eu/juris/document/document.jsf?text=&docid=184668&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=1062162