RESEARCH PAPER

Adapting Article 22 Of GDPR To The Indian Context: AI and Big Data

Pankaj Mishra [1*], Dr. Arunanshu Dubey [2]
[1*]Research Scholar, ILSR, GLA University, Mathura, Uttar Pradesh, India.
Email: mishrapankaj2726@yahoo.com
[2]Assistant Professor, Institute of Legal Studies & Research, GLA University, Mathura, Uttar Pradesh, India.
Email: arunanshu.dubey@gla.ac.in

ABSTRACT
The widespread adoption of artificial intelligence (AI) and big data analytics in sectors such as healthcare, finance, law enforcement, and employment raises pressing concerns about transparency, fairness, and individual rights. Article 22 of the European Union's General Data Protection Regulation (GDPR) provides a legal safeguard against decisions made solely through automated processing. This research examines how India, under its Digital Personal Data Protection Act, 2023 (DPDPA), can adapt and integrate similar protections. It explores the conceptual and regulatory gaps in the Indian framework and emphasizes the need for transparency, explainability, and accountability in AI-driven decision-making. Landmark cases such as *State of Wisconsin v. Loomis* and *Guerra v. Google LLC* illustrate the risks posed by opaque algorithms. In contrast, India's legal precedents like *KS Puttaswamy v. Union of India* and *Rajagopal v. State of Tamil Nadu* underscore the need for robust data protection and privacy safeguards. The study recommends a risk-based regulatory approach modeled after the EU AI Act, incorporating mechanisms such as human oversight, explainability, and bias audits. Ultimately, the paper advocates for a balanced strategy in India that fosters AI innovation while ensuring fundamental rights are protected against unjust automated decisions.
Keywords:AI, GDPR, Article 22, DPDPA 2023, Automation, Data Privacy, India
How to cite this article: Salieem S, Ahmed A. Emotional intelligence, self-efficacy and organizational commitment as moderators of work-life balance in organizations. Int J Drug Deliv Technol. 2026;16(3s): 867-873; DOI: 10.25258/ijddt.16.3s.105
.

INTRODUCTION

The rapid advancement and integration of artificial intelligence (AI), big data analytics, and machine learning technologies have revolutionized decision-making processes across critical sectors, including banking and finance, healthcare, policing, judicial systems, and employment. These technologies enable institutions to process vast datasets, identify patterns, and make swift decisions. However, the increasing reliance on automated decision-making mechanisms has simultaneously given rise to a spectrum of legal, ethical, and human rights concerns. Chief among these are issues of transparency, accountability, explainability, and the potential for discrimination or bias. Decisions that were once subject to human discretion and oversight are now often being rendered by opaque algorithmic systems, creating a "black box" effect where affected individuals have little to no understanding or control over outcomes that significantly impact their lives. In this context, regulatory frameworks must evolve to address the challenges posed by automated decision-making and ensure that technology serves society without compromising fundamental rights.

The European Union's General Data Protection Regulation (GDPR), which came into effect in 2018, includes Article 22—a provision that specifically addresses the right of individuals not to be subject to decisions based solely on automated processing, including profiling, where such decisions produce legal or similarly significant effects. Article 22 embodies a forward-thinking regulatory approach that acknowledges the risks inherent in unchecked algorithmic governance and establishes essential safeguards such as the right to human intervention, the right to express one's point of view, and the right to

obtain an explanation of the decision. It reflects a proactive model that aligns technological innovation with human rights protection and can serve as a blueprint for jurisdictions grappling with similar challenges. Countries across the globe have shown varying degrees of responsiveness to this issue. While the European Union has taken a clear stance with GDPR and the proposed AI Act, countries like the United States have adopted sector-specific, fragmented approaches. India, meanwhile, has enacted the Digital Personal Data Protection Act (DPDPA), 2023—a significant milestone in data privacy legislation. Yet, this Act does not explicitly address the challenges posed by automated decision-making, leaving a critical gap in the regulatory landscape.

This research paper critically analyzes the applicability of GDPR's Article 22 to the Indian context, with the objective of exploring how India can adapt similar legal safeguards within its own data protection and AI governance framework. The Indian legal landscape has,

*Author for Correspondence: mishrapankaj2726@yahoo.com

in recent years, undergone significant transformations, particularly following the Supreme Court's landmark ruling in *KS Puttaswamy v. Union of India* (2017), which declared the right to privacy as a fundamental right under Article 21 of the Indian Constitution. However, despite this judicial recognition of informational privacy and the enactment of the DPDPA, India lacks specific provisions addressing the fairness, accountability, and transparency of AI systems used in automated decision-making processes. The challenges are exacerbated by low public awareness, limited regulatory enforcement mechanisms, and the complexity of AI systems themselves. Therefore, this paper argues for a rights-based and risk-based regulatory model that bridges the existing legal vacuum and ensures that the development and deployment of AI in India are consistent with democratic values, constitutional guarantees, and global best practices.

Big data and data analytics artificial intelligence and machine learning have quite influenced decision-making aspects of specialized fields such as banking and finance, the healthcare sector, police and legal systems, and employment. These technologies have integration problems with transparency, equality, and individual rights.[1] Automated decision-making is regulated according to the GDPR Article 22, which focuses on the configuration of risks while providing transparency and reasonable choosing mechanisms with human participation. India has enacted the Digital Personal Data Protection Act, 2023 (DPDPA)[2] to establish a comprehensive data protection strategy, but lacks regulations like those outlined in GDPR Article 22. This paper explores how the GDPR's Article 22 might be implemented in India with an emphasis on protection against calculated decisions. It discusses the concept of understanding AI systems, decision-making opacity in relation to fairness, and innovation versus personal rights. The research considers the data protection framework of India to assess accountability and transparency and seeks to improve India's regulatory stance on and approach to AI and data protection.

GDPR ARTICLE 22 – AUTOMATED DECISION-MAKING AND SAFEGUARDS

Artificial intelligence (AI) embodies several aspirations and apprehensions, as well as problems and prospects. Numerous debates have occurred on the role of regulation in the development of AI and its use within society. This analysis examines Article 22 of the EU's GDPR, a European standard pertaining to automated decision-making.[3]

Art. 22 GDPR is a provision in French law that aims to align emerging technology with corresponding regulations. This progressive regulation reflects a "legislative dialogue" across international, European, and national law. The growth of automated decision regulation is noteworthy as it reflects a singular, continuous progression. Article 22 of the GDPR explains its essence by examining the evolution of legislation concerning new technologies and the stages involved in their progressive development and implementation. This approach aims to address the issue of reactive technology regulation and promote proactive regulation in the face of technological advancements.[4]

When first proposed in 1978 inside the French legal system, the plan to regulate computerized decision-making was groundbreaking. However, it was made available to all EU member states in accordance with EU law under Article 22 of the GDPR and Directive 95/46/EC.[5]

Finally, the member states of the Council of Europe's Convention 108 inserted the right of a person *"not to be subject to a decision significantly affecting him or her based solely on an automated processing of data without having his or her views taken into consideration".*[6]

1.1. Evolution of Automated Decision-Making and Profiling Protections under GDPR

This analysis explores Article 22 of the EU's GDPR, a European standard addressing automated decision-making. The GDPR aims to align emerging technology with corresponding regulations, reflecting a "legislative dialogue" across international, European, and national law. The growth of automated decision regulation is noteworthy, reflecting a singular, continuous progression. Article 22 aims to address reactive technology regulation and promote proactive regulation in the face of technological advancements.

The proposal to govern computerized decision-making was remarkable when first introduced in the French legal framework in 1978. Nonetheless, it was disseminated to all member states under European Union legislation via Directive 95/46/EC and Article 22 of the GDPR.

---

[1] Reuben Binns and Michael Veale "Is that your final decision? Multi-stage profiling, selective effects, and Article 22 of the GDPR." (2021) IDPL, 11(4), 319-332.

[2] Digital Personal Data Protection Act, Act No. 22 of 2023

[3] Florent Thouvenin, et al. "Article 22 GDPR on Automated Individual Decision-Making: Prohibition or Data Subject Right?" (2022) Eur. Data Prot. L. Rev., 8, 183.

[4] Filip Geburczyk, "Automated administrative decision-making under the influence of the GDPR–Early reflections and upcoming challenges." (2021) CLSR 41, 105538.

[5] Peter Hustinx, "EU data protection law: The review of directive 95/46/EC and the proposed general data protection regulation." (2013) University of Tartu. Data Protection Inspectorate, Tallinn.

[6] De Terwangne, C. "Council of Europe convention 108+: A modernised international treaty for the protection of personal data." (2021) CLSR, 40, 105497.

However, Article 9(1) of Modernised Convention 108 stipulates: *"Every individual shall have a right: (a) not to be subject to a decision significantly affecting him or her based solely on an automated processing of data without having his or her views taken into consideration; ... (c) to obtain, on request, knowledge of the reasoning underlying data processing where the results of such processing are applied to him or her; (d) to object at any time, on grounds relating to his or her situation, to the processing of personal data concerning him or her unless the controller demonstrates legitimate grounds for the processing which override his or her interests or rights and fundamental freedoms."*[7]

Data subjects' rights, freedoms, and legitimate interests may be protected by legislation that supports a controller's decision to exclude a right in Article 9(1)(a), as stated in Article 9(2). Legal precedent from the Council of Europe, including the "Recommendation on the Protection of Individuals with Regard to Automatic Processing of Personal Data in the Context of Profiling" (2010) and the 2017 Guidelines on the Protection of Individuals with Regard to Personal Data Processing in the Era of Big Data, as well as Articles 22 and 15 of the General Data Protection Regulation and Article 15 of the Data Protection Directive, inform these regulations.

1.2. The nature of the right in Article 22(1)

The "World Privacy Forum" (WP29) has argued that Article 22(1) of the GDPR should be a qualified ban, despite its right presentation. This interpretation maintains human participation safeguards and exceptions to consent and contract. However, this contradicts the explicit language of Article 22(1), which would have been articulated similarly to Article 22(4) or Article 11(1) if intended to establish a restriction. The prohibition-contra-right problem must be examined in the context of fully automated decision-making systems that conduct ex-ante "data protection impact assessment" (DPIA).[8]

1.3. Conditions for applying the right in Article 22

Article 22(1) of the GDPR confers upon persons the right to avoid decisions that are exclusively based on automated processing, including profiling, where such choices have legal or similarly important consequences. To exercise this right, three criteria must be fulfilled:[9]

(i) A judgment is rendered,
(ii) it is based only on automated processing, and
(iii) it has legal or substantial consequences for the person. These requirements closely mirror those in Article 15 of the Data Protection Directive (DPD) but with refined modifications under the GDPR.

Article 22 in Chapter III of the GDPR, designated "rights of the data subject," should be considered a right, but other elements are interpreted as obligations on controllers. The prohibition-contra-right issue must be considered in the context of fully automated decision-making systems, which must conduct a data protection impact assessment (DPIA) before implementing mitigating measures. If the DPIA shows a high risk and no measures have been taken to address it, the controller will have to inform the Data Protection Authority (DPA) and the latter may proceed under Article 58.[10]

TRANSPARENCY AND FAIRNESS IN AI-DRIVEN DECISION-MAKING

The growing utilization of AI in decision-making has elicited concerns regarding transparency and equity, particularly in the context of potential discrimination. This is largely due to the opacity of models, particularly those grounded in machine learning, which complicates the evaluation of their fairness, especially in sectors such as finance, employment, and criminal justice.

3.1. The incomprehensibility of AI Systems

The limited understandability due to the decision-making black box nature of the complex AI systems challenges the identifiability and traceability. The problem is that in such complex models like deep learning the decision-making process is not transparent and may produce biased or unfair results particularly when used in automated systems addressing individuals. A key example highlighting the risks of incomprehensible AI is the case of "*State of Wisconsin v. Loomis (2016)".*[11] Eric Loomis was forced into recidivism using a risk assessment tool known as COMPAS, which is an artificial intelligence. He said that due to a proprietary algorithm, he was unable to contest the results generated by the tool. In Wisconsin, the Supreme Court supports the use of COMPAS and points to issues of opacity and bias in the uses of AI in determining defendants' fate whereas they cannot contest the algorithms-generated decisions and predictions without disclosure.

3.2. Impact of AI Incomprehensibility on Fairness

[7] Greenleaf, Graham. "How far can convention 108+'globalise'? Prospects for Asian accessions." (2021) CLSR 40: 105414.

[8] Christian Djeffal, "The normative potential of the European rule on automated decisions: A new reading for Art. 22 GDPR." (2020) ZFAORV, 847-879.

[9] Bygrave, "Article 22 Automated individual decision-making, including profiling', in Christopher Kuner, and others (eds), The EU GDPR: A Commentary", <https://doi.org/10.1093/oso/9780198826491.003.0055>, accessed 10 October 2024.

[10] Kaminski, et al. "Multi-layered explanations from algorithmic impact assessments in the GDPR. Proceedings of the 2020 Conference on Fairness, Accountability, and Transparency." (2020).

[11] State of Wisconsin v. Loomis, 881 N.W.2d 749 (Wis. 2016).

A lack of understanding of AI systems tends to harm fairness as it may be challenging to identify cases of bias and rectify them in algorithms. Due to the reinforcement learning approach, the AI systems may periodically capture, strengthen, or even exacerbate bias that existed in historical data with the resultant prejudice impacting treatment based on color, gender, or any other protected category. In "*Guerra v. Google, LLC (2019)",*[12] A discrimination lawsuit was filed against Google for recruitment of candidates for the positions at the company. The case also pointed to the possibility of Google's AI recruitment tools performing similarly and excluding candidates based on demographic similarity; algorithms are known to perpetuate hiring bias as they screen for resumes containing features that match previous hires, for example, certain racial or gender profiles. While this case was able to be settled without going to court a specific concern of AI-driven systems is that such processes can perpetuate systemic bias if the mechanism behind the decision is not transparent.

3.3. Approaches to Overcoming AI Incomprehensibility

It is now possible to present decisions made by AI in such a manner that allows people to understand how specific predictions or recommendations have been reached without inflating their complexity or reducing their precision. This creates an ability for individuals to appreciate the rationale of results thereby making the process sensitive to human control. In Europe, the Right to Explanation under the GDPR gives the subject the right to obtain and understand explanations in case of decisions based on solely algorithms (Recital 71, Article 22). This right ensures that decision-making is not only transparent but also is done fairly; however, its practical application seems quite problematic because of the intricacy of AI models.[13] In India, the DPDPA also seeks to insert the principles of transparency in artificial intelligence decision-making. Yet, as India expands on its ever-evolving data protection mechanism, it must learn from global case laws and implement reasonable protection for the individual's rights in the proper evaluation and societal fairness and accountability framework.[14]

REGULATION OF AUTOMATED SYSTEMS: BALANCING INNOVATION AND RIGHTS

AI systems are in high levels of automation and therefore bring about concerns in relation to the law including the health, financial, and policing sectors. Thus, AI might bring in reform but challenges fundamental human rights such as privacy, the right against discrimination as well as right to a fair trial. Citizens' rights are still very important in the modern world and every country such as India needs to find the middle ground between technology and individual citizens' rights.[15]

4.1 Technological Innovation vs. Individual Rights

AI is being applied today in numerous decision-making processes which may have large consequences for individuals – work, credit, penalties, etc. But there is always the question of how such arrangements are going to be made without prejudicing the rights of citizens. The *"State of Wisconsin v. Loomis (2016)"*[16] clearly showed the danger of the implementation of the AI system in decision-making denying the voices of dominance for the oppressed gender. The United States is also facing this issue for predictive analytics in civil services which may challenge the fundamental rights of human beings as privacy and fair trial. There is the possibility of violating human rights due to the absence of restrictions regarding AI applications.

4.2 Global Approaches to AI Regulation

Across the world, there have been different mechanisms put in place to address AI and the use of automated decision-making. The GDPR in the European Union can be considered an example. In the GDPR, a person has a general right of non-automation under Article 22 especially where decisions are likely to have legal or similar effects. This regulation is one method of guaranteeing that baked into autonomous systems, there is human oversight so that individual liberty is upheld while at the same time accommodating advancements in advanced technology.[17]

The European Union has developed the Artificial Intelligence Act, which seeks to classify AI systems based on their risk level, imposing stricter controls on those used in high-risk sectors such as healthcare and law enforcement. Ensuring openness and equity while fostering innovation is a vital objective.[18]

Other nations, like as the United States, have not established a comprehensive federal regulation for AI;

[12] Guerra v. Google, LLC, No. 5:2019cv00570 (N.D. Cal. 2019).

[13] Emre Bayamlıoğlu, "The right to contest automated decisions under the General Data Protection Regulation: Beyond the so-called "right to explanation"." Regulation & Governance 16.4 (2022), 1058-1078.

[14] Fatema Motiwala, "Comparative Study of General Data Protection Regulation (GDPR) and Digital Personal Data Protection Act (DPDP): A Way Out for European Industry to Navigate through Indian Personal Data Protection Regulation." (2024).

[15] Wiedemann, Klaus. "Profiling and (automated) decision-making under the GDPR: A two-step approach." (2022) CLSR 45: 105662.

[16] State of Wisconsin v. Loomis, 881 N.W.2d 749 (Wis. 2016).

[17] Emre Bayamlıoğlu, "Transparency of automated decisions in the GDPR: an attempt for systemisation." (2018) SSRN 3097653.

[18] Fink, M. "The EU Artificial Intelligence Act and access to justice." (2021) EU Law live, 1-4.

instead, some regulations pertain to the sector-specific use of AI in such as healthcare and finance. This strategy offers freedom and innovation; nonetheless, it has shortcomings, such as insufficient protection of individual rights in unregulated firms. [19]

ACCOUNTABILITY AND TRANSPARENCY IN INDIA'S AI-DRIVEN DECISION-MAKING FRAMEWORK

India is at a pivotal moment in its approach to AI and automated decision-making, following the Philippines' proposed Digital Personal Data Protection Act, 2023 (DPDPA). India can learn from foreign experiences and integrate them into its socio-economic and legal environment. The Indian Supreme Court's landmark case, KS Puttaswamy v. In Union of India (2017), has declared the Right to Privacy as a fundamental right, emphasizing the need for privacy, transparency, and accountability in AI regulation. This will guide India's approach to AI regulation.

5.1 India's Data Protection Framework: DPDPA

The DPDPA, 2023 is India's first attempt to increase legal restraints and personal data protection, focusing on purpose limitation, consent, and accountability for data processing. However, it lacks clear provisions for AI decision-making, particularly regarding automated decisions, transparency, and explainability. AI systems often act on large amounts of personal data, leading to potential errors in denying services, sorting individuals, prejudice, or invading privacy. The KS Puttaswamy case established India's constitutional right to privacy, which serves as the foundation for the data protection system. The case emphasizes privacy, dignity, and individual decision-making, particularly in the context of AI systems processing personal data. It emphasizes the importance of respecting human rights, providing accountability, and transparency in decision-making processes, particularly in the context of AI systems.[20]

5.2 Challenges for Accountable AI in India

Perhaps one of the most critical issues in the Indian context concerning AI is that AI systems are black boxes. Most AI systems that are based on machine learning algorithms, for example, work in capture mode where the final decision made as to what is correct is not explainable. The opacity also becomes an impediment to how one can challenge or seek redress where they end up on the receiving end of an unfair decision by AI systems, as afforded by numerous countries and territories' case laws including the *State of Wisconsin v. Loomis (2016)*[21] where the defendant apparently could not comprehend the AI-based risk assessment tool used in his sentencing. Furthermore, India has numerous contextual issue that includes low awareness of AI technologies among the public, poor regulation, and inadequate digital platforms. The above challenges inhibit processes that seek to make AI systems accountable and transparent to society.

5.3 Ensuring Transparency and Accountability in AI-Driven Decisions

The following changes should be adopted to increase transparency and accountability of tilted decisions made by AI in Indian law: First, any AI operating on the lives of people—healthcare, justice, or banking, for example—requires strict levels of transparency. It would include a precise description of how a decision is being taken, what information is being relied on, and how clandestine bias risks are managed.

The case of "*Rajagopal v. State of Tamil Nadu" (1994)*[22] which developed an individual's right to privacy in the course of state espionage, strengthens the requirement for organizations that organize personal data. This judgment is not about AI itself, however, it supports the concept of the data subject's right to information about data processing concerning him and his right to object to data-driven decisions.

However, descriptive measures in India should also implement provisions like GDPR, usually, Article 22 which asserts that citizens cannot be subjected to decisions solely based on automated procedures. This right would allow persons who are impacted by decisions made by AI to appeal to humans to challenge decisions that have an impact on their rights.

CONCLUSION

The rapid proliferation of artificial intelligence (AI) and big data technologies across diverse domains—such as healthcare, finance, policing, and employment—has necessitated a re-evaluation of existing legal frameworks to ensure the protection of individual rights and democratic values. While the transformative potential of AI is undeniable, its increasing integration into decision-making processes, particularly those that bear legal or similarly significant consequences, demands regulatory scrutiny. In this context, Article 22 of the General Data Protection Regulation (GDPR) offers a pertinent legal safeguard by granting individuals the right not to be subject to decisions based solely on automated processing. This right is especially critical when such decisions affect an individual's legal status, access to opportunities, or entitlements. However, despite India's recent enactment of the Digital Personal Data Protection Act, 2023 (DPDPA), there remains a conspicuous absence of

[19] Gaviria, Carlos Ignacio Gutierrez. "The role of artificial intelligence in pushing the boundaries of US regulation: A systematic review." (2022) SCHT. LJ 38, 123.

[20] Naithani, P. "Analysis of India's Digital Personal Data Protection Act, 2023." (2024) IJLM

[21] State of Wisconsin v. Loomis, 881 N.W.2d 749 (Wis. 2016).

[22] Rajagopal v. State of Tamil Nadu, (1994) 6 SCC 632.

comparable protections that address the risks inherent in AI-driven decision-making.

The Indian data protection regime, though a step in the right direction, lacks the specificity and enforceable safeguards provided under the GDPR, particularly Article 22. India must recognize that the black-box nature of AI systems—characterized by their opacity, incomprehensibility, and lack of explainability—poses a significant challenge to individual autonomy, transparency, and the right to fair treatment. The inability to trace the logic behind algorithmic decisions makes it difficult to detect biases or errors and renders any form of redress ineffective. This concern is not merely theoretical but has been evidenced in global legal precedents such as *State of Wisconsin v. Loomis*, where the use of an opaque AI tool (COMPAS) significantly influenced judicial sentencing without the defendant's ability to contest its findings. Similarly, in *Guerra v. Google LLC*, algorithmic hiring practices came under scrutiny for perpetuating discrimination. These cases highlight the urgent need for legal mechanisms that prioritize transparency, human oversight, and fairness in AI deployments.

India's legal landscape already acknowledges the significance of privacy and data protection through landmark judgments like *KS Puttaswamy v. Union of India*, which upheld privacy as a fundamental right. This judicial recognition should form the bedrock of AI regulation in India. Additionally, precedents such as *Rajagopal v. State of Tamil Nadu* reiterate the individual's right to information and consent in data processing. These principles must be expanded to cover automated decision-making, thereby bridging the gap between technological innovation and constitutional rights.

To achieve this, India must consider integrating a legal provision analogous to Article 22 of the GDPR within its data protection framework. This would ensure that individuals are not subject to automated decisions without human intervention, particularly in high-stakes domains. Furthermore, India must adopt a risk-based approach akin to the EU's Artificial Intelligence Act, which classifies AI applications by risk level and imposes proportionate obligations. High-risk AI systems—such as those used in criminal justice or healthcare—should be subject to stringent requirements, including impact assessments, explainability mandates, and human review mechanisms. At the same time, measures should be taken to promote innovation through regulatory sandboxes, public-private partnerships, and funding for AI research aligned with ethical principles.

While India stands at the threshold of a data-driven future, the regulatory architecture must evolve to ensure that technological advancements do not come at the expense of individual rights. A harmonized legal framework that balances innovation with accountability, drawing on international best practices like Article 22 of the GDPR, is imperative for fostering trustworthy AI in India.

REFERENCES

I. Statutes and Regulations

1. Digital Personal Data Protection Act, Act No. 22 of 2023 (India).
2. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (General Data Protection Regulation – GDPR).
3. Council of Europe, Convention 108+, Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, as modernized.

II. Case Laws

1. *State of Wisconsin v. Loomis*, 881 N.W.2d 749 (Wis. 2016).
2. *Guerra v. Google, LLC*, No. 5:2019cv00570 (N.D. Cal. 2019).
3. *Rajagopal v. State of Tamil Nadu*, (1994) 6 SCC 632 (India).
4. *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1 (India).

III. Books and Commentaries

1. Lee A. Bygrave, "Article 22 Automated Individual Decision-Making, Including Profiling," in *The EU GDPR: A Commentary*, Christopher Kuner et al. (eds), Oxford University Press, 2020, [https://doi.org/10.1093/oso/9780198826491.003.0055].

IV. Journal Articles and Conference Proceedings

1. Reuben Binns & Michael Veale, *Is that your final decision? Multi-stage profiling, selective effects, and Article 22 of the GDPR*, 11(4) *Int'l Data Privacy L.* 319–332 (2021).
2. Florent Thouvenin et al., *Article 22 GDPR on Automated Individual Decision-Making: Prohibition or Data Subject Right?*, 8 *Eur. Data Prot. L. Rev.* 183 (2022).
3. Filip Geburczyk, *Automated Administrative Decision-Making under the Influence of the GDPR–Early Reflections and Upcoming Challenges*, 41 *Computer L. & Security Rev.* 105538 (2021).
4. Peter Hustinx, *EU Data Protection Law: The Review of Directive 95/46/EC and the Proposed General Data Protection Regulation*, University of Tartu, Data Protection Inspectorate (2013).
5. Caroline De Terwangne, *Council of Europe Convention 108+: A Modernised International Treaty for the Protection of Personal Data*, 40 *Computer L. & Security Rev.* 105497 (2021).
6. Graham Greenleaf, *How Far Can Convention 108+ 'Globalise'? Prospects for Asian Accessions*, 40 *Computer L. & Security Rev.* 105414 (2021).
7. Christian Djeffal, *The Normative Potential of the European Rule on Automated Decisions: A New Reading for Art. 22 GDPR*, *ZFAORV* 847–879 (2020).

8. Emre Bayamlıoğlu, *The Right to Contest Automated Decisions Under the General Data Protection Regulation: Beyond the So-Called "Right to Explanation"*, 16(4) *Regulation & Governance* 1058–1078 (2022).
9. Emre Bayamlıoğlu, *Transparency of Automated Decisions in the GDPR: An Attempt for Systemisation*, *SSRN* (2018), [https://ssrn.com/abstract=3097653].
10. Kaminski et al., *Multi-Layered Explanations from Algorithmic Impact Assessments in the GDPR*, in *Proceedings of the 2020 Conference on Fairness, Accountability, and Transparency* (2020).
11. Fatema Motiwala, *Comparative Study of General Data Protection Regulation (GDPR) and Digital Personal Data Protection Act (DPDP): A Way Out for European Industry to Navigate Through Indian Personal Data Protection Regulation*, (2024).
12. Klaus Wiedemann, *Profiling and (Automated) Decision-Making Under the GDPR: A Two-Step Approach*, 45 *Computer L. & Security Rev.* 105662 (2022).
13. Michael Fink, *The EU Artificial Intelligence Act and Access to Justice*, *EU Law Live* (2021).
14. Carlos Ignacio Gutierrez Gaviria, *The Role of Artificial Intelligence in Pushing the Boundaries of US Regulation: A Systematic Review*, 38 *SCHT. L.J.* 123 (2022).
15. P. Naithani, *Analysis of India's Digital Personal Data Protection Act, 2023*, *Indian Journal of Law & Management* (2024).