International Journal of English Literature and Social Sciences
Vol-10, Issue-5; Sep-Oct, 2025

Peer-Reviewed Journal
Journal Home Page Available: https://ijels.com/
Journal DOI: 10.22161/ijels

A Right to Reasonable Inferences: Re-Thinking Data Protection Law in the Age of Big Data and AI

Ashikur Rahman

Master of Information Technology, Department of Computer Engineering, Belhaven University, Jackson, Mississippi
Orcid: 0009-0006-8069-2271

Received: 25 Sep 2025; Received in revised form: 21 Oct 2025; Accepted: 26 Oct 2025; Available online: 29 Oct 2025

Abstract— *The advent of Big Data analytics and artificial intelligence (AI) has fundamentally altered the data processing landscape. The data-driven systems of today can make probabilistic inferences about individuals, predicting their characteristics, behaviors, and likely future actions. They are no longer restricted to using and collecting raw data. This paper argues that the core tenets of data protection law, particularly the EU's General Data Protection Regulation (GDPR), are inadequately equipped to address the novel risks posed by inferential analytics. While the GDPR provides a robust framework for raw data, its application to inferences remains ambiguous and underdeveloped. Through systematically examining the GDPR's rights and obligations and analyzing the ECJ's jurisprudence, this paper demonstrates that inferences frequently fall into a regulatory gray area. The current legal framework struggles with inferences' subjectivity, verifiability, and qualification as personal data. As a result, essential rights like access, rectification, and objection are frequently rendered useless. This paper proposes a paradigm shift: recognizing a distinct "right to reasonable inferences." This right would consist of two core components: (1) a substantive principle requiring that inferences meet thresholds of acceptability, relevance, and reliability, and (2) a procedural right to contest inferences deemed unreasonable effectively. Finally, the paper suggests ways to strike a balance between the rights of data subjects and the legitimate interests of data controllers, addressing intellectual property and trade secrets law as a significant obstacle to such a right.*

Keywords— ***Data Protection, GDPR, Inferences, Artificial Intelligence, Machine Learning, Big Data, Reasonable Inferences, Privacy, Fundamental Rights, Intellectual Property.***

I. INTRODUCTION

The economy of inferences is the digital economy. In the age of Big Data and artificial intelligence (AI), the primary value is no longer derived solely from the raw data collected from individuals—their clicks, purchases, locations, and stated preferences. The sophisticated analytical procedures that process this data to generate new knowledge—predictions, classifications, profiles, and assumptions about individuals that they may not even be aware of themselves—confer the transformative power. A financial technology company infers our creditworthiness from our social network and typing speed; a hiring platform infers our potential from patterns in our CV and voice tone; and a streaming service infers our mood from our viewing history. These inferences, powered by complex machine learning models, shape life-altering opportunities in employment, finance, healthcare, and justice.

European data protection law, culminating in the General Data Protection Regulation (GDPR), represents the world's most ambitious attempt to regulate the processing of personal data and protect the fundamental rights and freedoms of natural persons. Together with a set of individual rights, its principles of lawfulness, fairness, transparency, purpose limitation, and data minimization form a comprehensive framework for giving individuals control over their personal data. However, this framework was primarily conceived in a pre-Big Data era, focused on processing factual, provided, or observed data.

The central argument of this paper is that, despite its effectiveness, the General Data Protection Regulation (GDPR) does not adequately address the difficulties posed by inferential analytics. The law's architecture is predicated on a model of data processing where the data in question is objective, verifiable, and directly linked to an individual. By nature, inferences are probabilistic, subjective, and frequently unproven. They are predictions about what a person is or might do, not facts about what they did. This creates a fundamental tension at the heart of data protection law.

This paper will argue that data protection law must be rethought and explicitly extended to include a right to reasonable inferences to meet the challenges of the algorithmic age. This is not merely a call for stricter enforcement of existing rules but a proposal for a new legal principle that directly addresses the qualitative nature of inferences themselves. The paper will proceed as follows. Part II will explore the paradigm shift from explanations to inferences, detailing the novel risks of inferential analytics and formally introducing the right to reasonable inferences concept. Part III will delve into whether inferences can even be considered "personal data" under the law, analysing the ECJ's three-step model and the challenges of subjectivity and verifiability. Part IV will provide a detailed analysis of the relevant jurisprudence of the European Court of Justice in cases such as YS and M and S and Nowak, extracting crucial lessons on the remit of data protection law concerning inferences. The practical efficacy of rights to access, rectification, objection, and erasure, as well as special protections for sensitive inferences, will be evaluated in Part V by systematically examining the GDPR's current protections against inferences. Part VI will formally propose the right to reasonable inferences, outlining its two core components: a justification requirement and a robust contestation mechanism. Finally, Part VII will address a significant practical barrier to implementing this right—the conflict with intellectual property law and trade secrets—and propose pathways to a necessary balance.

II. EXPLANATIONS TO REASONABLE INFERENCES

The digital revolution has precipitated a move from a world of documented facts to probabilistic predictions. Traditional data processing involved recording and organising facts: an address, a salary, a purchase transaction. The individual's relationship with this data was often direct and understandable; they could confirm or deny its accuracy. The fair and accurate handling of this recorded reality was the function of data protection law. This model is destroyed by inferential analytics. In this case, the input data are merely the foundation upon which a brand-new, inferred reality is built. This inferred reality is not a record of the past but a prediction of the future or an assessment of a hidden present.

The Novel Risks of Inferential Analytics and a Right to Reasonable Inferences

The ability to infer introduces a new category of risks difficult to mitigate under current data protection guidelines: Opacity and Complexity: The algorithms that generate inferences, intense learning models, are often "black boxes." Even their creators are sometimes unable to fully explain why a particular inference was drawn for a particular person. This opacity directly undermines the GDPR's principles of transparency and fairness, as well as the right to an explanation.

The Problem of Verifiability: How does one verify an inference? If a system infers that Person A has a 85% probability of defaulting on a loan, what constitutes "accurate" data? The inference is a probability, not a fact. It cannot be proven "true" or "false" in a binary sense until a future event occurs—and even then, the fact that the person did not default does not necessarily mean the inference was "wrong"; it might have been a correct assessment of a 15% chance of non-default. Rights like rectification face fundamental difficulties as a result of this. Reiteration of Discrimination and Bias: Inferences do not arise in a vacuum. They are learned from training data from the past. If this data reflects societal biases (e.g., historical hiring discrimination against women), the model will learn to infer that being a woman is a negative predictor for hireability, thus perpetuating and automating discrimination at scale. The inference itself becomes a vehicle for bias.

Moral and Autonomy Harm: Inferences can create a "digital double" of an individual—a profile that may not align with their self-perception or identity. When decisions are made based on this digital double, it can lead to a loss of autonomy and self-determination. A person's ability to determine their own life path may be restricted if they are denied a loan because of an algorithmic inference about their "type." Chilling Effects: Self-censorship and a conformist chilling effect, in which people avoid exploring ideas or activities that could lead to undesirable inferences, can result from the awareness that one's behavior is constantly being analyzed and classified. These risks demonstrate that the harm is no longer just about the misuse of data we provide, but about the construction of knowledge we never agreed to. The current GDPR framework, which focuses on data processing, is analogous to regulating factory ingredients but not finished goods. The inference—the output—is where the actual impact is. A new focus is required as a result: a right to reasonable inferences. This right posits that the act of concluding an individual is not a value-neutral, technical process but one that must be subject to normative constraints. **It shifts the question from "Was the raw data processed lawfully?" to "Is the inference itself reasonable and fair?"**

A right to reasonable inferences would encompass both procedural and substantive elements. Procedurally, it would guarantee individuals meaningful transparency into the logic of significant inferences and a practical ability to challenge them. It would logically entail responsibilities for data controllers to ensure that the inferential processes they use adhere to specific standards of dependability, relevance, and acceptability in a democratic society. It is a right that seeks to govern the quality of the conclusions drawn about us, not just the process of how they were drawn.

III. INFERENCES PERSONAL DATA?

This document applies to the application of the GDPR's extensive obligations, which is triggered by one crucial condition: the processing of "personal data." Article 4(1) defines personal data as "any information relating to an identified or identifiable natural person." The crucial term is "information relating to." The gateway question for determining whether the GDPR apparatus applies is whether an inference falls within this definition.

A. Step-by-Step Method

A framework for interpreting "relating to" has been developed by the European Court of Justice and the Article 29 Working Party (WP29), which was followed by the European Data Protection Board (EDPB). This is often conceptualised as a three-step test:

Content: Is the information about a person? Does it reveal anything about that person? An inference such as "high credit risk" clearly refers to an individual. Purpose: Is the information used or likely to be used to evaluate, treat, or analyse a person in a certain way? The very purpose of an inference is to assess an individual for decision-making, easily satisfying this element.

Consequently, does the individual's use of the information affect their rights and interests? Given that inferences are used to make significant decisions, the result is almost always a potential impact.

Applying this test, most inferences would comfortably qualify as personal data. A credit score is information about a person (content), is used to decide on loan applications (purpose), and certainly impacts the individual's financial opportunities (result). The same logic applies to inferred interests for advertising, inferred health risks, or inferred job performance.

B. Subjectivity and Verifiability

The legal challenge arises not from the "relating to" test but the nature of the "information" itself. The GDPR's regime, particularly the rights of access (Article 15) and rectification (Article 16), implicitly assumes that personal data is largely objective and verifiable. An individual can access their data and request its correction if it is inaccurate. An address can be checked; a transaction can be confirmed.

Inferences defy this model. They are subjective conclusions, not objective statements of fact. They are a likelihood or probability. This creates a profound tension:

Access: A data subject has the right to "meaningful information about the logic involved" in automated decision-making under Article 15(1)(h). But what does "meaningful" mean for a complex neural network? Providing a list of the thousands of weighted variables is meaningless to a human. The right to access the "data" itself is complicated when the data is an inference. Does the controller have to disclose the inferred probability score?

Rectification: Article 16 provides the right to rectification of inaccurate personal data. However, how can an inference be corrected? If a model infers "person X is likely to commit fraud," what would rectification entail? A forced speech that interferes with the controller's analysis would move the controller to change the inference to "not likely." The data subject could argue that the underlying data is inaccurate, but the inference might be a mathematically correct output from that (flawed) data. The problem is the model, not the data point.

This subjectivity and non-verifiability create a risk that inferences, while technically falling under the definition of personal data, operate in a practical limbo where the core rights designed to protect individuals are difficult, if not impossible, to exercise effectively. The law recognises them as data but lacks the tools to manage their unique characteristics.

IV. JURISPRUDENCE OF THE EUROPEAN COURT OF JUSTICE

The ECJ's rulings provide essential guidance on navigating the boundaries of data protection law, particularly concerning inferences and the nature of personal data.

A. Joined Cases C-141/12 and C-372/12: YS and M and S

This case concerned a third-country national's request for access to the legal analysis contained in a Dutch immigration authority's file, which was used to reject his residence application.

1. Inferences as Personal Data

The Court made a crucial distinction. The final decision (the rejection) was unquestionably personal data. However, the internal legal analysis—the notes, reasoning, and inferences made by the caseworker applying law to fact—was not considered personal data. The Court reasoned that this analysis did not constitute "information" about the applicant but was "information about the assessment and application of that law by the administration." It was an opinion about how the law applied to the facts, not a point about the applicant himself.

This is a highly formalistic and narrow interpretation. It suggests that pure analytical constructs, even if they directly and solely concern an individual and determine their fate, might be placed outside the scope of the definition of personal data if they are framed as "legal advice" or "internal analysis." This creates a potential loophole where controllers could argue that their algorithmic inferences are merely internal analytical models, not personal data in their own right.

2. Remit of data protection law

The ruling in YS underscores a traditional, limited view of the remit of data protection law: its primary concern is factual data about an individual, not the mental or analytical processes applied to that data. This view is ill-suited to the AI age, where the analytical method is the source of the new, impactful data (the inference). If a machine's "analysis" is afforded the same protection as a human's legal advice, the GDPR's applicability to algorithmic inferences is severely weakened.

B. Case C-434/16: Nowak

In contrast, the Nowak case offered a more expansive interpretation. It concerned a candidate's request to access his corrected exam answers under the Data Protection Directive (the GDPR's predecessor).

1. Inferences as Personal Data

The ECJ held that the written answers, the comments of the examiner, and the marks awarded all constituted personal data. Crucially, the Court stated that personal data "covers any information concerning the data subject" and that this "reflects the aim of the [GDPR] to ensure a high level of protection of the fundamental rights and freedoms of natural persons." The answers revealed the candidate's knowledge and intellect, and the examiner's comments reflected an evaluation (an inference) of his performance.

2. Remit of Data Protection Law

Nowak takes a much more expansive and goal-oriented approach. The key question is not the formal label of the information (e.g., "legal analysis" vs. "exam answer") but whether it relates to and affects the individual. The examiner's comments are inferences and evaluations, yet they were brought within the scope of data protection law because they were integral to a decision affecting the individual.

C. Lessons from Jurisprudence of the ECJ

The tension between YS and Nowak reveals the ongoing struggle of traditional legal concepts to adapt to new technological realities.

The Form vs. Substance Dilemma: YS prioritises the form of the information (internal analysis), while Nowak prioritises its substance and effect (evaluation of an individual).

A Narrow vs. Broad Remit: YS suggests a narrower remit for data protection law, potentially excluding analytical outputs. Nowak advocates for a broad, rights-centric remit that encompasses evaluative information.

The Human vs. Machine Problem: The reasoning in YS might be defensible for a human caseworker's internal musings. However, applying the same logic to a machine's output is dangerous. A machine does not have "internal thoughts"; its output is the data product. To exclude algorithmic inferences from the definition of personal data because they are "internal analysis" would be to create a catastrophic loophole.

The correct path forward, aligned with the Charter of Fundamental Rights and the GDPR's objective of ensuring a high level of protection, is to follow the Nowak rationale. The output of an algorithmic process—the inference—must be considered personal data if it is used to evaluate an individual or make decisions about them. Its status cannot depend on being a "final decision" rather than an "intermediate analysis." In an algorithmic system, the inference is the decision-making currency.

V. PROTECTION AGAINST INFERENCES UNDER DATA PROTECTION LAW

Assuming that inferences are recognised as personal data, the next question is how effectively the GDPR's existing rights and obligations protect individuals from the risks they pose.

A. The Right to Know About Inferences

Article 15 provides the right of access. For inferences, this right has several components:

Right to access the inference itself: The data subject should be able to know what has been inferred about them (e.g., "your inferred credit risk score is 650").

Right to meaningful information about the logic (Art. 15(1)(h)): This is critical. The individual must be explained how the inference was reached.

The practical implementation of Article 15(1)(h) is the subject of intense debate. Does "meaningful information" necessitate the algorithm's full disclosure? This could certainly not infringe on IP and reveal trade secrets. Does it require a simple, high-level description? This would be not very sensible. The emerging consensus leans towards a "functional explanation": an explanation that describes the main factors that contributed to the inference in a way that is understandable to the data subject. For example, "Your loan application was rejected primarily due to your high debt-to-income ratio and the short length of your credit history." While this does not reveal the algorithm's inner workings, it does provide useful information. However, for highly complex models, even providing a functional explanation that is both accurate and non-technical remains a significant technical and legal challenge. The right to know, therefore, while necessary, is often insufficient on its own.

B. The Right to Rectify Inferences

Article 16 provides the right to rectification of inaccurate personal data. This is where the nature of inferences creates its greatest challenge.

What does it mean for an inference to be "inaccurate"? One can distinguish two scenarios:

Inaccuracy in underlying data: If an inference is based on factually incorrect raw data (e.g., an incorrect late payment mark on a credit report), the path to rectification is clear: correct the underlying data, which should, in a well-functioning system, lead to a corrected inference.

Inaccuracy in the inference itself: This is the core problem. If the underlying data is correct, but the inference is perceived as unfair, biased, or wrong, can it be "rectified"? For instance, if a model correctly uses shopping data (bought pregnancy vitamins) to infer a woman is pregnant, but she is not, the inference is inaccurate. However, from a statistical perspective, the model performed correctly—it made a high-probability inference based on a strong correlate.

Rectifying this is not a simple matter of correcting a fact. It may require:

Appending a supplementary statement: The individual could have the right to add a note to their profile contesting the inference ("Subject has confirmed she is not pregnant").

Deletion of the inference: Treating the inference as data in its own right and requesting its erasure under Article 17.

Changing the model: Changing the biased or flawed model that led to the inference may be the real solution, not changing just one inference. However, Article 16 does not easily impose an obligation on a controller to retrain their entire AI system for one individual.

The right to rectification, as currently framed, is a blunt instrument for the nuanced problem of inaccurate inferences.

C. The Rights to Object to and Delete Inferences

1. Right to Object (Article 21): This right allows an individual to object to processing based on legitimate interests or public task. The controller must then stop processing unless it demonstrates compelling legitimate grounds. This could be a potent weapon against marketing or profiling inferences. An individual could say, "I object to you inferring my political opinions for ad targeting." However, the right is not absolute and can be overridden by the controller's compelling interests.

D. Protections against Sensitive Inferences

1. Can personal inferences be considered sensitive data? Article 9 prohibits the processing of special categories of personal data (e.g., data revealing racial origin, political opinions, health, etc.) unless an exception applies. A critical question is whether an inference can fall under this prohibition. Data "revealing" these characteristics is mentioned in the text of Article 9. This suggests that an inference ought to be treated as sensitive data itself if it is intended to reveal a sensitive characteristic or has the effect of doing so. For example, an inference that someone is "likely to have diabetes" or "likely a socialist" is data revealing health or political opinions and should trigger the strict protections of Article 9. This is a powerful application of the law: it means that creating sensitive inferences is presumptively unlawful unless a specific exemption is met.

2. Reliability and intention The complication arises with unintentional or unreliable inferences. What if an output that is correlated with a health condition is produced by a model that was not designed to infer health? Or what if the inference is highly unreliable? The GDPR does not require the processing to be intentional or reliable for Article 9 to apply. If the data reveals (or is used to treat someone as if it reveals) a sensitive characteristic, the prohibition is triggered. This places a high burden on controllers to ensure their models do not inadvertently generate sensitive inferences.

E. The Right to Challenge Inference-Based Decisions Articles 21 and 22 provide specific rights regarding automated decision-making, including profiling. Article 22(1) establishes the general right "not to be subject to a decision based solely on automated processing... which produces legal effects or similarly significantly affects him or her." This is a crucial right directly aimed at the risks of inferences.

When such a decision is made, Article 22(3) mandates the right to "obtain human intervention on the part of the controller, to express his or her point of view and to contest the decision." This right to contest is a cornerstone of protection. It acknowledges that the fairness of the outcome may be the issue rather than the accuracy of the data.

However, its limitations are notable:

It only applies to solely automated decisions. Many systems use automation as a recommendation for a human, circumventing the article.

Procedural rights grant contest rights. It does not guarantee a particular outcome, only a right to be heard.

It only addresses the decision that was based on the inference, not the reasonableness of the inference itself.

VI. RE-ALIGNING THE REMIT OF DATA PROTECTION LAW IN THE AGE OF BIG DATA: A RIGHT TO REASONABLE INFERENCES

A regulatory void is revealed by the above analysis. The GDPR applies to inferences, but the tools it uses aren't suited to them. As a new interpretative principle and potential future legal reform, we propose the recognition of a freestanding right to reasonable inferences. As a direct normative standard for the act of inference itself, this right would complement and enhance the existing framework. This right would have two core, interdependent components:

A. Justification to Establish Acceptability, Relevance, and Reliability

The first component is substantive. Any significant inference used in decision-making would need to be justifiable as reasonable. Three factors would be used to determine this justifiability: Acceptability: The inference must be morally and socially acceptable. It should not be based on protected characteristics or lead to impermissible discrimination, even if it is statistically "accurate." An inference about a person's health from their grocery shopping may be reliable, but could be deemed unacceptable due to its intrusive nature and the risk of harm. Data analytics now has a moral boundary thanks to this criterion. Relevance: The inference must be relevant and proportionate to the specific context and purpose for which it is used. The data and model used must have a verifiable and substantial connection to the outcome being predicted. Using inferred personality traits from social media to assess creditworthiness likely fails the relevance test, as the link is tenuous and unproven.

Reliability: A reliable, statistically sound, and empirically validated method must be used to draw the inference. It should be up to the controller to show that the model has been tested for accuracy and bias and is good enough for the job at hand. A "black box" model whose reliability cannot be demonstrated would fail this test.

This justification requirement would flip the current dynamic. Instead of the individual having to prove an inference is "inaccurate" (a near-impossible task), the controller would have a positive duty to ensure and demonstrate that its inferences are acceptable, relevant, and reliable before deploying them in a way that affects individuals.

B. Contestation of Unreasonable Inferences

The second component is procedural. It would create a strengthened, dedicated right for individuals to contest inferences they believe to be unreasonable, going beyond the contestation of decisions under Article 22.

This contestation process would involve:

A clear avenue for individuals to lodge a challenge against a specific inference or a type of inference.

a requirement for the controller to respond to a challenge with a more comprehensive explanation of the inference, possibly involving external auditors to verify claims without disclosing trade secrets. A meaningful review process. This could involve a dedicated internal role (e.g., an "Algorithmic Review Officer") or an easy path to refer the challenge to a data protection authority.

Meaningful remedies. If an inference is found to be unreasonable, the controller should be obliged to not only delete or correct that inference but also to review and amend the model to prevent similar unreasonable inferences in the future.

Together, the justification requirement and the contestation mechanism would create a system of accountability focused on the quality and impact of inferences, finally giving practical effect to the GDPR’s principles of fairness and accountability in the age of AI.

VII. BARRIERS TO A RIGHT TO REASONABLE INFERENCES: IP LAW AND TRADE SECRETS

A formidable barrier to implementing transparency and contestation rights is the conflict with the protection of intellectual property (IP) and trade secrets. The algorithmic model of a business is frequently its most valuable asset, and disclosing its inner workings could destroy the competitive advantage of the business.

A. Algorithmic Models and Statistical Purposes in the GDPR

The GDPR itself acknowledges this tension. Processing for "archiving purposes in the public interest, scientific or historical research purposes or statistical purposes" is protected by Article 89. The development of AI models could be framed as a "statistical purpose." "insofar as it should be subject to appropriate safeguards for the rights and freedoms of the data subject," the GDPR should not apply to personal data processed for statistical purposes, as stated in recital 162. This could be interpreted to limit data subject rights, including access, in the context of model development.

Nevertheless, this is not a complete exemption. When the model is used to make decisions about individuals, it becomes operational rather than just "statistical." The protections for data subjects must then come first. At this stage of the deployment, the right to reasonable inferences would be most applicable.

B. Algorithmic Models and the EU's Trade Secrets Directive

The EU's Directive on the protection of undisclosed know-how and business information (Trade Secrets Directive) protects information that is secret, has commercial value because it is secret, and has been subject to reasonable steps to keep it secret. Algorithmic models squarely fit this definition.

Controllers will inevitably argue that disclosing information about the logic of inferences under Article 15 or during a contestation process would reveal their trade secrets. The GDPR does not override the Trade Secrets Directive. "Including trade secrets or intellectual property," according to GDPR's recital 63, "the right of access should not adversely affect the rights or freedoms of others."

C. Balancing and proportionality in conflict resolution.

The solution is not to allow IP law to trump fundamental rights, but to find a balance. Data protection authorities and courts must engage in a careful balancing test, weighing the data subject's fundamental right to protection against the controller's economic interests. Several techniques can achieve this balance without disclosing core IP:

Functional Explanations: As mentioned, providing explanations of the key factors behind a decision without revealing their precise weighting or the algorithm's code.

Audited Compliance: Requiring controllers to have their models audited by independent third parties who can verify claims of accuracy, fairness, and the absence of bias without publicly disclosing the model's details. The auditor's certificate could be provided to the data subject and authority.

Strict Necessity and Proportionality: Any disclosure required for a contestation should be limited to what is strictly necessary. A data subject may only require evidence that a particular problematic variable was not used, rather than the entire algorithm.

Confidentiality Procedures: Implementing procedures for DPA officials or judges to review algorithms in-camera (in private) to adjudicate a claim without making the information public.

The right to reasonable inferences must be designed with this balance in mind. It cannot demand full algorithmic transparency. Even in the presence of legitimate trade secrets, it must instead demand accountability, which can be accomplished through effective contestation and verified justification.

VIII. CONCLUSION

This document The rise of inferential analytics represents a quantum leap in the power of technology to shape human lives. The General Data Protection Regulation (GDPR), which embodies data protection law, provides a solid foundation of principles and rights, but it is showing its age when faced with the particular difficulties of probabilistic inference. In spite of treating inferences as a unique type of personal data, the current framework does not provide the specialized tools necessary to guarantee that they are equitable, non-discriminatory, and subject to meaningful human control. Through an analysis of the ECJ's jurisprudence, we see a legal system grappling with the boundaries of its own concepts. Through a systematic review of the GDPR's rights, we see that while avenues for protection exist, they are often difficult to navigate and ineffective against the core problem of unreasonable inference.

The path forward requires a paradigm shift. The right to reasonable inferences is a new right fit for a world of predictions that requires us to move beyond a framework designed for a world of recorded facts. This right would establish that the act of drawing conclusions about individuals is not a free exercise but must be justified against standards of acceptability, relevance, and reliability. It must be coupled with a robust and practical right to contest.

Inevitably, this right will clash with the economic interests embedded in intellectual property law. However, trade secrets cannot be used to silence fundamental rights. A balance must be struck through innovative governance solutions like audited compliance and functional explanations.

Re-thinking data protection law in the age of Big Data and AI is not an optional academic exercise; it is a necessary endeavour to preserve human autonomy, dignity, and fairness in the face of increasingly powerful technologies. Embedding a right to reasonable inferences into our legal fabric is the crucial next step in this ongoing evolution.

ACKNOWLEDGEMENTS

The authors would like to thank Belhaven University for the research.

REFERENCES

[1] R. Aslan, *No god but God: The origins, evolution, and future of Islam*. New York: Random House, 2005.

[2] J. L. Esposito, *Islam: The straight path* (3rd ed.). Oxford: Oxford University Press, 1998.

[3] T. Ramadan, *In the footsteps of the Prophet: Lessons from the life of Muhammad*. Oxford: Oxford University Press, 2007.

[4] N. A. Rahman, "AI at War: The next revolution for military and defense," *World Journal of Advanced Research and Reviews*, vol. 27, no. 1, pp. 1998–2004, 2025. doi: 10.30574/wjarr.2025.27.1.2735.

[5] L. Ahmed, *Women and gender in Islam: Historical roots of a modern debate*. New Haven, CT: Yale University Press, 1992.

[6] K. Armstrong, *Islam: A short history*. New York: Modern Library, 2000.

[7] A. Rahman, A. Jony, M. Hosen, M. Priya, and Y. Arafat, "Information Technology Perspective on Business," *International Journal for Multidisciplinary Research*, vol. 7, no. 4, 2025. doi: 10.36948/ijfmr.2025.v07i04.53765.

[8] S. H. Nasr, *The heart of Islam: Enduring values for humanity*. New York: HarperOne, 2002.

[9] E. W. Said, *Orientalism*. New York: Pantheon Books, 1978.

[10] O. Roy, *Globalized Islam: The search for a new ummah*. New York: Columbia University Press, 2004.

[11] F. Mernissi, *The veil and the male elite: A feminist interpretation of women's rights in Islam*, M. J. Lakeland, Trans. Reading, MA: Addison-Wesley, 1991.

[12] J. A. C. Brown, *Misquoting Muhammad: The challenge and choices of interpreting the Prophet's legacy*. London: Oneworld Publications, 2014.

[13] C. Kurzman, Ed., *Liberal Islam: A sourcebook*. Oxford: Oxford University Press, 1998.

[14] R. W. Hefner, *Civil Islam: Muslims and democratization in Indonesia*. Princeton, NJ: Princeton University Press, 2000.

[15] A. R. Nazil, "AI-Powered Visualization is Transforming Modern Healthcare," *International Journal of Research Publication and Reviews*, vol. 6, no. 8, pp. 1474–1478, 2025.

[16] A. Rahman, "AI-Powered Visualization is Transforming Modern Healthcare," *International Journal for Multidisciplinary Research*, vol. 7, no. 4, 2025. doi: 10.36948/ijfmr.2025.v07i04.53087.

[17] P. Mandaville, *Transnational Muslim politics: Reimagining the umma*. London: Routledge, 2001.

[18] A. R. Nazil, "The GENIUS Act and the Future of Stablecoins: Balancing Innovation, Regulation, and Financial Stability," *figshare. Journal contribution*, 2025. doi: 10.6084/m9.figshare.29602880.v1.

[19] A. R. Nazil, "A Comparative Analysis of Technological Trajectories in the United States and Japan," *figshare. Journal contribution*, 2025. doi: 10.6084/m9.figshare.29369222.v1.

[20] A. R. Nazil, "Black magic effect technology: Understanding the Reality, Risks, and Remedies of Magic in Islamic Teachings," *figshare. Journal contribution*, 2025. doi: 10.6084/m9.figshare.29389832.v1.

[21] A. R. Nazil, "AI-Powered Visualization is Transforming Modern Healthcare," *figshare. Journal contribution*, 2025. doi: 10.6084/m9.figshare.29877074.v1.

[22] A. R. Nazil, "AI-Powered Visualization is Transforming Modern Healthcare," *figshare. Journal contribution*, 2025. doi: 10.6084/m9.figshare.29876651.v1.

[23] A. R. Nazil, "Mastering Complexity: How AI Will Control and Transform the IT Industry by 2040," *figshare. Journal contribution*, 2025. doi: 10.6084/m9.figshare.29364962.v1.

[24] J. R. Bowen, *A new anthropology of Islam*. Cambridge: Cambridge University Press, 2012.

[25] H. A. Agrama, *Questioning secularism: Islam, sovereignty, and the rule of law in modern Egypt*. Chicago, IL: University of Chicago Press, 2012.

[26] Future AI cryptocurrency. (n.d.). https://crajour.org/articles/300

[27] Sani, J. (n.d.). "Waste Management in Bangladesh: Current practices, challenges and policy directions." Zenodo. https://doi.org/10.5281/zenodo.16894330