Revista de Științe Politice. Revue des Sciences Politiques • No. 90 • 2026: 56 – 66

ORIGINAL PAPER

The legal challenges of artificial intelligence in data and consumer law

Armand Mihail Calotă[1)]

Abstract:
The integration of Artificial Intelligence into contemporary commercial strategies has opened a new chapter in the balance of power between economic operators and consumers. Analyzing the legal vulnerabilities that arise at the intersection of technological innovation and fundamental rights of the individual, we discover two essential pillars, namely the protection of personal data and the integrity of consent. Exploring the risks that artificial intelligence systems pose to the General Data Protection Regulation (GDPR) and analyze the phenomenon of invisible data collection, where profiling algorithms can infer sensitive information without a clear legal basis, defying the principle of transparency and purpose limitation. Nowadays, data is the new oil, traditional protection mechanisms seem increasingly difficult to apply in the face of algorithms that process information at superhuman speeds.
Thus, our research focuses on deceptive commercial practices enhanced by artificial intelligence. Dark patterns and personalized pricing algorithms are examined, which can manipulate consumer decision-making by exploiting automatically identified cognitive biases. We can ask a legal question: where does legitimate personalization end and where does misleading begin? The analysis aims at the need to adapt consumer protection legislation to include legal liability for autonomous acts of AI systems, going beyond simple human error. We underline the urgency of a hybrid regulatory framework, which harmonizes the new European regulations (AI Act) with existing legislation and which argues that real consumer protection in the digital age cannot be achieved without a rigorous algorithmic audit and without reaffirming the right to human intervention, thus ensuring that technological progress is not achieved by sacrificing data security and the citizen's freedom of choice.
Keywords: *Artificial intelligence (AI), algorithmic management, dark patterns, GDPR compliance, informed consent.*
JEL Classification: K24, K13

[1)] Lecturer, Ph.D., University of Craiova, Faculty of Law, Department of Public Law and Administrative Sciences, Craiova, Romania.

1. Introduction

Artificial intelligence now shapes many commercial interactions, from the advertisements people see to the prices, recommendations, and contract terms presented to them online, and this expansion has intensified legal concerns about privacy, fairness, and the real freedom of consumer choice. In the European legal order, these concerns are not marginal, because AI systems often rely on profiling, automated decision-making, and large-scale data processing that directly engage GDPR safeguards and consumer-protection rules against misleading or unfair practices.

Digital markets no longer operate only through visible offers and explicit negotiations. Increasingly, commercial decisions are shaped in the background by algorithmic systems that observe behaviour, classify users, predict preferences, and adapt interfaces in ways that are not always perceptible to the individual concerned. This matters legally because a consumer may appear to act freely while, in reality, the surrounding digital environment has already been tailored to influence attention, accelerate consent, or steer the final decision in a commercially advantageous direction.

From the perspective of data protection law, the first difficulty lies in the fact that AI systems do not merely collect data that users knowingly provide. They can also generate new information through inference, correlation, and profiling, sometimes revealing highly sensitive aspects of a person's life even where such data was not expressly disclosed at the outset. This creates tension with core GDPR principles such as transparency, fairness, purpose limitation, and lawful processing, because the person concerned may not understand what is being processed, for what purpose, or with what consequences.

From the perspective of consumer law, the second difficulty concerns the growing capacity of AI to refine commercial influence. The issue is no longer limited to ordinary advertising, but it also concerns interface design, behavioural targeting, and personalized commercial strategies that may exploit cognitive vulnerabilities and distort economic choice. Dark patterns are especially relevant here, because they show how a digital architecture can be designed not simply to inform the consumer, but to direct behaviour in subtle ways that may qualify as misleading or unfair under European consumer law.

A central legal tension therefore emerges between legitimate personalization and unlawful manipulation. Personalization is not, in itself, prohibited in European law, yet it becomes problematic when it relies on opaque profiling, when it interferes with informed consent, or when it materially impairs the consumer's ability to take a free and informed transactional decision. The real challenge is to determine the point at which technological optimization ceases to serve consumer convenience and begins instead to undermine autonomy, equality, and trust in the digital marketplace.

This discussion becomes even more important in light of the new European regulatory framework on artificial intelligence. The AI Act strengthens the language of risk management and human oversight, especially for high-risk systems, and confirms that technical innovation cannot be separated from the protection of fundamental rights. Read together, the GDPR, consumer-protection law, and the AI Act suggest that effective protection in the digital economy depends not only on formal compliance, but also on meaningful transparency, accountable system design, and the possibility of human intervention where automated processes significantly affect individuals.

For that reason, the introduction should guide the reader toward a simple but important idea about how AI has changed the mechanics of market influence, while the

law is still adapting its traditional concepts to this new reality. What is at stake is not only the legality of data processing, but also the preservation of genuine consumer autonomy in an environment increasingly shaped by invisible technological choices.

2. Challenges to GDPR principles

The growing reliance on artificial intelligence for data-driven decision-making has brought the core principles of European data protection law under renewed pressure. In particular, the GDPR must now operate in an environment where personal data are continuously generated, inferred, and re-combined by complex models whose technical logic is often opaque even to their developers. Legal doctrine has therefore started to focus not only on classical issues such as consent and purpose limitation, but also on structural questions of accountability, explainability and risk management in AI-based processing.

Specialized literature emphasizes that AI systems challenge the foundational principles of lawfulness, fairness and transparency that structure GDPR compliance. Studies on profiling and big data show that automated analysis of large datasets can reveal detailed behavioural patterns and sensitive traits with remarkable precision, raising doubts as to whether individuals can still meaningfully understand and control the use of their personal information. At the same time, policy-oriented work underlines the need for clearer guidance on how AI applications can remain compatible with the GDPR without sacrificing their innovative potential.

A first point of tension between AI systems and the GDPR concerns profiling and the creation of inferred data. Profiling is understood in European law as any form of automated processing used to evaluate personal aspects of an individual, in particular to analyse or predict elements such as performance at work, economic situation, health, personal preferences, interests or behaviour. Literature on tax, financial and marketing profiling shows that AI systems routinely derive additional information from apparently innocuous data points, reconstructing highly detailed profiles that can be used for risk scoring, targeted advertising or eligibility assessments (Politou et al., 2019).

This indirect and largely invisible data collection stands in tension with the principle of transparency, which requires that data subjects receive clear, intelligible information about the nature, purposes and consequences of processing. When AI infers, for example, sensitive health or emotional information from online behaviour or biometric signals, individuals may not even be aware that such categories have been constructed, much less that they are being evaluated on that basis. Legal commentators therefore warn that the traditional model of informed consent (based on discrete, clearly explained processing operations) does not fully reflect the reality of continuous, exploratory data analytics that characterize many AI systems.

The principle of purpose limitation is also affected. GDPR requires that personal data be collected for specified, explicit and legitimate purposes and not further processed in a manner incompatible with those purposes. Yet the economic logic of AI encourages re-use of existing datasets for new, unforeseen applications, including further training of models, cross-context profiling or development of new predictive products. Voigt et al., (2017) analysing AI governance in the EU and Romania underline that organisations often underestimate the constraints imposed by purpose limitation and tend to assume that data collected for one business purpose can later be used for AI in general, an assumption that is incompatible with GDPR doctrine.

The question of lawful bases for AI-driven processing is now central in both academic and practitioner discussions. Analyses of GDPR compliance for AI stress that many controllers seek to rely on legitimate interests when training or deploying AI models, although this ground presupposes a careful balancing between the controller's interests and the fundamental rights of data subjects. Where AI systems produce significant effects on individuals, such as credit decisions, dynamic pricing or eligibility for essential services, several authors argue that a more demanding legal basis (such as explicit consent or specific legislative authorization) may be required to satisfy GDPR standards (European Commission, 2016).

The debate is particularly sharp around Article 22 GDPR, which limits decisions based solely on automated processing that produce legal effects or similarly significant impacts on individuals. Legal scholarship and institutional reports point out that AI-based systems often approach, or even cross, this threshold in sectors such as employment, financial services and consumer contracting. Recent doctrinal work examines whether the narrow list of exceptions in Article 22 contract necessity, explicit consent and authorization by law, offers sufficient protection in an era where automated decision-making can be built into everyday digital interactions, including consumer-facing platforms and personalized online environments.

European guidance on automated decision-making and profiling reiterates that data subjects must be informed not only of the existence of automated decisions, but also of the logic involved, as well as the significance and envisaged consequences of such processing. However, specialized literature highlights a gap between these information duties and the technical reality of complex, often opaque machine-learning models, where even developers may struggle to provide a concise and meaningful explanation of how a particular output was generated (Kaminski et al., 2021). This explains the growing importance of research on algorithmic impact assessments and multi-layered explanations designed to translate technical processes into legally relevant information.

Beyond formal legality, Montinaro (2024) insist on the substantive dimension of fairness in AI-based data processing. Contributions to the debate on GDPR and AI underline that even where a nominal legal basis exists, automated profiling can still reproduce or intensify social inequalities, for example by incorporating historically biased data or by optimising for commercial objectives that conflict with vulnerable consumers' interests. Work on emotion recognition and personalized advertising illustrates how AI-driven inferences about emotional states or psychological traits can be used to target individuals in highly sensitive situations, raising questions about undue influence and exploitation of vulnerabilities.

This has led to increased attention to discrimination risks, particularly in contexts where AI systems classify or rank individuals for access to credit, employment or essential services. While anti-discrimination law operates alongside data protection, the GDPR's own emphasis on fairness and data minimisation provides an additional normative basis for questioning data practices that systematically disadvantage certain categories of individuals. European and national reports on AI governance note that regulators are beginning to expect bias mitigation, documentation and impact assessment as part of the accountability obligations imposed on controllers deploying high-impact AI systems.

At the same time, studies of AI in financial services and tax administration, including work with a Romanian focus, highlight the tension between efficiency and rights protection. On one hand, AI promises more accurate risk assessment, fraud

detection and service personalization and on the other, these applications intensify monitoring and expand the collection and analysis of personal data, reinforcing the asymmetry of information and power between institutions and individuals (Mitrache et al., 2025). This broader structural imbalance is central to understanding why formal consent or information notices may not suffice to guarantee real autonomy in data-driven environments.

One of the central themes in academic debate is accountability. Under the GDPR, controllers must be able to demonstrate compliance with data-protection principles, a duty that takes on new complexity when decisions are generated by autonomous or semi-autonomous AI. Scholarship on GDPR-compliant AI argues that accountability requires not only legal documentation, but also technical and organisational measures such as data-protection impact assessments, algorithmic audits, clear allocation of responsibilities in AI supply chains and effective channels for individuals to contest or obtain human review of automated decisions.

Closely linked to accountability is the demand for explainability. Legal and interdisciplinary work on algorithmic explanations suggests that explanations may need to operate on multiple levels: technical (for auditors and experts), legal (for supervisory authorities) and user-facing (for data subjects and consumers). Without some degree of intelligibility, rights such as access, rectification, objection or the right to obtain human intervention remain largely theoretical in AI-driven environments. This explains the interest in methods that translate complex model behaviour into understandable narratives about the main parameters, data sources and decision criteria involved in specific AI applications.

In this context, Romanian-focused studies on AI, data protection and digital governance underline that national authorities, such as the National Supervisory Authority for Personal Data Processing (ANSPDCP), play a key role in operationalising these European standards. Research on AI in Romanian economic and public-sector settings emphasises the need for clear institutional guidance, sector-specific impact assessments and capacity-building to ensure that GDPR and AI-related obligations are effectively implemented rather than remaining purely declaratory (Francu et al., 2025).

3. AI-Driven consumer manipulation

The use of AI in digital markets has intensified concerns about manipulative commercial practices, particularly through dark patterns and personalized pricing that exploit behavioural data and cognitive biases rather than simply informing the consumer. In European doctrine, these practices are increasingly analysed through the lens of consumer autonomy, rather than purely through traditional information and transparency models.

The term dark patterns describes interface designs and choice architectures that steer users towards specific outcomes (subscribing, sharing more data, accepting tracking) by taking advantage of predictable cognitive biases. In EU law scholarship, authors show that such patterns sit on the boundary between legitimate persuasion and unlawful manipulation, because they do not merely present information, but structurally distort the decision-making environment (Brenncke, 2024).

Studies on dark patterns in EU consumer law, notably by Roșca (2024), argue that these practices are already addressable under the Unfair Commercial Practices Directive (UCPD), the Consumer Rights Directive (CRD) and the Unfair Contract Terms Directive (UCTD), even though the term *dark patterns* do not yet appear expressly in all

instruments. The emerging view is that dark patterns often materially distort the economic behaviour of the average consumer or of vulnerable groups, which is the key criterion for unfairness under EU consumer law.

At the same time, recent work develops a theory of exploitation for consumer law, arguing that many dark patterns must be understood as behavioural exploitation rather than mere deception. Leiser and Santos (2023) emphasise that online choice architectures can systematically leverage biases, time pressure or information overload to obtain choices that consumers would not reasonably have made in a neutral environment. In this perspective, the key legal question is whether a design undermines autonomy, not simply whether it conveys technically accurate information.

Digital-policy analyses by organisations such as BEUC and the European Parliament underline this shift by calling for an explicit principle of digital fairness and, in some proposals, fairness-by-design obligations that would require traders to structure interfaces in ways that support, rather than undermine, informed and free consumer choice.

European Parliament (2022) studies and academic work on personalized pricing note that such systems often fall through the cracks of the current legal framework. They typically do not qualify as high-risk AI under the AI Act, so strict obligations on logging, auditing and human oversight may not apply, even though the techniques resemble other high-risk applications, such as those used for credit scoring. As a result, UCPD standards on misleading and aggressive practices, combined with GDPR rules on profiling and automated decisions, become the main tools for controlling AI-driven pricing strategies.

From a conceptual standpoint, the literature converges on a delicate line, personalization is acceptable when it supports relevance and convenience, for example, by recommending products genuinely aligned with a consumer's interests, while it becomes problematic when it systematically exploits information asymmetries and hidden profiles to extract maximum value from each user. The autonomy-based approach to exploitation proposed in consumer law scholarship suggests that the legality of an AI-based practice should depend on whether it respects or undermines the consumer's capacity for self-determination, rather than on whether it increases short-term economic efficiency.

Against this background, the role of AI in dark patterns and personalized pricing illustrates the broader tension in European consumer law identified in works such as AI and Consumer Protection in the Cambridge Handbook of the Law, Ethics and Policy of AI (2025): *the traditional model of the rational, well-informed consumer is increasingly inadequate in a digital environment where choices are shaped by continuous, data-driven optimisation*. This explains why many authors now argue for a hybrid framework, where consumer-protection law, data-protection law and the AI Act are interpreted together to address both informational and behavioural dimensions of digital manipulation.

4. Liability and regulatory gaps in autonomous AI systems

The question of liability becomes especially difficult when harm is produced through autonomous or semi-autonomous AI systems, because the traditional model of liability is built around a relatively clear human act, a foreseeable causal chain, and an identifiable fault. In the AI context, however, opacity, adaptive behaviour and distributed decision-making make it much harder to determine who actually caused the harm: the

developer, the provider, the deployer, the trader using the system, or the human who formally approved the final output.

Recent doctrine rightly observes that the EU AI Act is not, in itself, a liability instrument. It is mainly an ante regulatory framework, focused on risk classification, compliance duties, technical documentation and human oversight, especially for high-risk systems. As Fink (2025) shows in the literature on Article 14 AI Act, human oversight is conceived as a safeguard for fundamental rights, but this does not automatically solve the downstream question of civil responsibility once damage has already occurred.

This is where an important regulatory gap appears. The current European model tends to separate prevention from compensation. The AI Act seeks to reduce risks before deployment, while liability remains dispersed across the revised Product Liability Directive, national tort law, contract law, and sector-specific rules. As several authors note, this fragmented architecture creates uncertainty for victims, because an injured person may still face serious obstacles in proving fault, causation and access to evidence, especially when the relevant system functions as a technical black box.

The debate surrounding the AI Liability Directive made this difficulty particularly visible. Garcia (2024) and other recent commentators have emphasized that the proposed directive was meant to ease the burden of proof, notably through disclosure mechanisms and presumptions of causation in certain cases. Even if the proposal was seen as imperfect, the doctrine generally agrees that ordinary national liability rules are poorly adapted to AI harms, precisely because opacity and autonomy make classical fault-based litigation unusually burdensome for the injured party.

A second gap concerns the fact that not all harmful AI systems fall within the high-risk categories of the AI Act. Some systems may produce serious economic or discriminatory effects in consumer markets without formally triggering the most demanding obligations under the Act. This means that important practices (especially in digital contracting, behavioural targeting or price personalization) may remain only partially governed by AI-specific rules, even though their impact on individuals can be substantial.

In this area, a convincing doctrinal position is that liability should not depend on recognising AI as a legal person. Most contemporary authors rejects the idea of electronic personhood and instead favours responsibility being attached to the actor who controls, benefits from, or deploys the system in practice. That approach is preferable, because granting legal personality to AI would risk weakening accountability rather than strengthening it.

From a normative point of view, the best reading of current EU developments is that compliance alone is not enough. A trader may formally satisfy documentation and risk-management duties, yet consumers can still suffer harm through biased outputs, opaque scoring, or automated refusals that are difficult to challenge in practice. For that reason, liability in the AI field should move toward a more coherent framework in which meaningful human oversight, auditability, access to explanation, and easier redress mechanisms operate together rather than separately (Falelakis et al., 2026).

So the real weakness of the present framework is not the absence of regulation, but the absence of a fully integrated bridge between technical compliance and effective private-law remedies. In that sense, the law still reacts to AI as if prevention and compensation were distinct worlds, although, in reality, genuine protection requires both.

5. Toward a hybrid regulatory framework

The previous analysis shows that no single branch of law can adequately address the risks created by AI in digital markets. Data protection law focuses on lawful processing, transparency and individual rights, while consumer law addresses misleading practices and distortion of economic behaviour, and the AI Act adds an ante model of risk governance and human oversight. Taken separately, each of these instruments is useful, taken together, they reveal the need for a hybrid regulatory framework capable of responding to AI as both a technical system and a market power tool.

This integrated perspective is also visible in the work of Spulbar (2025), who argues that AI-driven markets require flexible legal systems able to preserve innovation without undermining market integrity, accountability and data governance. The contribution is relevant here because it situates AI not only as a matter of compliance, but as a structural force reshaping algorithmic trade, autonomous decision-making and data-guided business models. In that sense, it is normal to support a broader doctrinal conclusion, that regulation must move beyond isolated legal silos and address the economic architecture within which AI operates.

A convincing regulatory model should therefore rest on at least three complementary pillars. First, algorithmic transparency must be strengthened, not only through formal disclosures, but through meaningful explanations that allow consumers and authorities to understand the logic, purpose and likely effects of AI-driven processing. Second, algorithmic audit and documentation should become a normal governance requirement in areas where AI influences contractual, commercial or pricing decisions, because hidden optimisation systems cannot be effectively supervised without traceability. Third, the right to human intervention should be reaffirmed in practice, not treated as a symbolic safeguard, particularly where automated decisions significantly affect consumer choice or access to services.

From a normative standpoint, the most important point is that real consumer protection in the digital economy cannot rely exclusively on information duties. Consumers are often placed in environments designed to shape their behaviour before any conscious legal choice is made, which means that legal protection must also address the architecture of influence itself (Santos et al., 2025). This is why a hybrid framework should combine the rights-based logic of the GDPR, the fairness-oriented logic of consumer law, and the preventive logic of the AI Act.

One of the persistent weaknesses of the current European approach is that the applicable rules are spread across several instruments, interpreted by different authorities, and enforced through partially distinct procedures, which can generate fragmentation and uncertainty for both individuals and market actors. In matters involving AI, this institutional fragmentation is particularly problematic because the same practice may simultaneously raise issues of data protection, consumer manipulation, automated decision-making and market fairness.

For this reason, effective protection in AI-driven markets should also include a stronger culture of regulatory coordination. Data protection authorities, consumer protection bodies and market surveillance institutions should not operate in isolation when examining AI-based commercial conduct, because the legal effects of these systems are rarely confined to a single field of law. A more coordinated model of supervision would make it easier to identify systemic risks, especially where

manipulative design, opaque profiling and automated commercial decisions overlap in ways that remain difficult to capture through a single legal lens.

Another important element concerns the transformation of legal protection from a purely reactive model into a more preventive one. It is no longer sufficient for the law to intervene only after harm has occurred, since AI systems can shape behavior continuously, subtly and at scale. In this field, prevention means anticipating risks through impact assessments, explainability requirements, human review mechanisms and auditable system design before consumer harm becomes widespread and normalized.

At a deeper level, the debate on AI and consumer law is also a debate about the type of digital economy that European law is prepared to accept. If innovation is understood only in terms of efficiency, speed and predictive accuracy, then the legal system risks tolerating forms of commercial influence that gradually empty consent and autonomy of real substance. If, by contrast, innovation is linked to trust, accountability and respect for fundamental rights, then legal regulation becomes not an obstacle to technological development, but a condition for its legitimacy.

The central conclusion that emerges is therefore a simple one: the legal response to AI cannot remain compartmentalized. The protection of personal data, the fairness of commercial practices and the accountability of automated systems are no longer separate problems, because in digital markets they increasingly arise through the same technological processes. A coherent response requires not only new rules, but also a unified legal understanding of how AI reorganizes the relationship between trader, consumer and data.

Seen in this light, the future of consumer protection in the digital economy will depend on whether the law can preserve a meaningful space for human agency. The real objective is not to resist technological progress, but to ensure that efficiency does not replace freedom, and that personalization does not become a refined form of invisible control. Only under these conditions can AI remain compatible with the values that European private law and fundamental-rights law are meant to protect.

References:

Brenncke, M. (2024). A theory of exploitation for consumer law: Online choice architectures, dark patterns, and autonomy violations. J. Consumer Pol'y, 47, 127.

Falelakis, T., Dimara, A., & Anagnostopoulos, C. N. (2026). Systemic Data Bias in Real-World AI Systems: Technical Failures, Legal Gaps, and the Limits of the EU AI Act. Information, 17(4), 326. https://doi.org/10.3390/info17040326

Fink, M. (2025). Human oversight under article 14 of the EU AI act. Available at SSRN. http://dx.doi.org/10.2139/ssrn.5147196

Francu, C. C., & Ștefan, S. A. V. A. (2025). Global Perspectives on Digital and AI Legislation: A Comparative Study of Data Protection, AI Governance, and Healthcare Innovations with a Focus on Romania. In Proceedings of the International Conference on Business Excellence (Vol. 19, No. 1, pp. 2469-2481). Sciendo.

Garcia, B. (2024). The regulation of AI liability in Europe: a critical overview of two recent directive proposals–the (new) AILD and the (revised) PLD. e-Publica, 11(3). https://doi.org/10.47345/v11n3art3

Kaminski, M. E., & Malgieri, G. (2021). Algorithmic impact assessments under the GDPR: producing multi-layered explanations. International data privacy law, 11(2), 125-144.

Leiser, M., & Santos, C. (2023). Dark patterns, enforcement, and the emerging digital design acquis: Manipulation beneath the interface.

Mitrache, L. A., & Spulbar, L. F. (2025). The Role of Artificial Intelligence in Promoting Economic Sustainability and Resilience. Revista de Stiinte Politice, (88), 235-245.

Montinaro, R. (2024). Emotion Recognition and Personalized Adverting. European Review of Private Law, 32(6). https://doi.org/10.54648/erpl2025012

Politou, E., Alepis, E., & Patsakis, C. (2019). Profiling tax and financial behaviour with Big Data under the GDPR. *Computer law & security review*, *35*(3), 306-329. https://doi.org/10.1016/j.clsr.2019.01.003

Rosca, C. (2024). Digital Arms for Digital Consumer Harms: Mapping Legal and Technical Solutions for Dark Patterns in EU Consumer Law.

Santos, C., Morozovaite, V., & De Conca, S. (2025). No harm no foul: how harms caused by dark patterns are conceptualised and tackled under EU data protection, consumer and competition laws. Information & Communications Technology Law, 34(3), 329-375.

Spulbar, L. F. (2025). Legal frameworks for AI-driven markets and their challenges and opportunities in the digital economy. Revista de Științe Politice. Revue des Sciences Politiques, (86), 288-304.

Voigt, P., & Von dem Bussche, A. (2017). The eu general data protection regulation (gdpr). A practical guide, 1st ed., Cham: Springer International Publishing, 10(3152676), 10-5555.

*** The Cambridge Handbook of the Law, Ethics and Policy of AI. (2025). https://www.cambridge.org/core/books/cambridge-handbook-of-the-law-ethics-and-policy-of-artificial-intelligence/ai-and-consumer-protection/F5F0BBC5ABC0318DD902417C07482F6B

*** European Commission. (2016). Are there restrictions on the use of automated decision-making? https://commission.europa.eu/law/law-topic/data-protection/rules-business-and-organisations/dealing-citizens/are-there-restrictions-use-automated-decision-making_en

*** European Parliament. (2022). Personalised Pricing. https://www.europarl.europa.eu/RegData/etudes/STUD/2022/734008/IPOL_STU(2022)734008_EN.pdf

Article Info

Received: April 29 2026
Accepted: June 20 2026

How to cite this article:

Calotă, A. M. (2026). The legal challenges of artificial intelligence in data and consumer law. *Revista de Științe Politice. Revue des Sciences Politiques,* no. 90, pp. 56-66.