Revista de Științe Politice. Revue des Sciences Politiques • No. 87 • 2025: 48 – 58

ORIGINAL PAPER

The impact of automated decisions on consumers. Legal and ethical challenges in the AI era

Armand Mihail Calotă[1)]

Abstract:
As artificial intelligence (AI) continues to influence consumer engagement, models for automated decision-making are transforming the commercial landscape. Whether credit evaluation, individualized pricing, or anti-fraud measures, AI-augmented methodologies are yielding efficiencies along with presenting considerable legal and ethical complexities. This article delves into the intersection of AI and consumer law, analyzing the effects of automated decision-making on consumer rights, data privacy concerns, and fairness.
As artificial intelligence holds the potential to augment customer experiences, it also threatens algorithmic bias, opacity, and possible breaches of data protection regulations. Typically, customers may have limited possibilities for redress against algorithmic decisions made by non-transparent algorithms that provide them with limited choice, which challenges the conventional legal frameworks. Consequently, policymakers and regulators are therefore struggling with ways to promote accountability, avoid discrimination, and uphold consumer protection amidst this fast-developing environment.
This article addresses key legal issues, such as the applicability of current consumer protection legislation, the development of AI regulation, and business obligations in AI governance. It mentions recent case studies illustrating instances in which AI-generated decisions have harmed consumers, thereby underlining the necessity of regulatory disclosure and the ethical development of AI technologies. It further examines possible solutions, including explainable AI models, fairness testing, and more robust enforcement mechanisms for protecting consumer rights.
As artificial intelligence increases its presence in consumer markets, it is essential to make sure that computerized decision-making rests on legal as well as ethical foundations. The appropriate equilibrium between innovation and consumer protection will necessitate constant cooperation between governments, business firms, and attorneys to develop an even and equitable AI-driven economy.

Keywords: *Automated decision-making, consumer protection, AI regulation, consumer law, ethical AI.*

[1)] Lecturer, Ph.D., University of Craiova, Faculty of Law, Department of Public Law and Administrative Sciences, Craiova, Romania, Email: avocati_comercial@yahoo.com

The impact of automated decisions on consumers.
Legal and ethical challenges in the AI era

1. Introduction

The proliferation of artificial intelligence (AI) across economic and social sectors has profoundly reshaped the dynamics between businesses and consumers. As companies increasingly adopt algorithmic systems to inform and automate decisions, the traditional contours of consumer protection law are being tested in unprecedented ways. From credit scoring and loan approvals to personalized pricing and fraud detection, AI-driven technologies are no longer auxiliary tools but have become central instruments in how consumers are evaluated, classified, and targeted in the marketplace.

These automated decisions, often rendered through opaque algorithms with minimal human oversight, pose significant legal challenges. One of the most pressing concerns relates to the principle of transparency, a cornerstone of many legal systems aiming to safeguard individuals against arbitrary or discriminatory treatment. When consumers are subjected to algorithmic decisions, especially those with substantial effects such as, being denied credit or offered differential pricing they are frequently unaware of the criteria used or even that an automated process has taken place. This lack of transparency impedes their ability to seek redress or challenge decisions, conflicting with well-established procedural rights recognized under instruments such as the EU's General Data Protection Regulation (GDPR), particularly Article 22, which grants individuals protection against decisions based solely on automated processing that produce legal or similarly significant effects.

Moreover, automated decision-making raises intricate questions of fairness and non-discrimination, principles embedded not only in data protection law but also in consumer protection frameworks. The use of AI systems trained on historical or biased data can lead to the reproduction (or even amplification) of societal inequalities, disadvantaging certain consumer groups based on race, gender, geography, or socioeconomic status. This contradicts the obligations of fairness and good faith in business-to-consumer transactions, reflected in regulations such as the EU's Unfair Commercial Practices Directive (2005/29/EC), which aims to shield consumers from deceptive and aggressive market behavior.

From a legal standpoint, these developments also complicate the attribution of responsibility. When harm results from an automated decision, identifying the liable actor becomes challenging. The algorithm may have been developed by one entity, deployed by another, and trained on data collected by a third. Traditional legal constructs, such as fault-based liability and consumer contract doctrines, are often ill-equipped to address this distributed responsibility and the technical opacity involved. This fragmentation undermines the efficacy of consumer remedies and erodes legal certainty, which are both essential components of a fair marketplace.

Furthermore, the deployment of AI in consumer contexts intersects with emerging regulatory landscapes that are still in flux. Legislative initiatives such as the EU Artificial Intelligence Act signal an attempt to classify and regulate AI systems according to their risk levels, with specific obligations for high-risk applications, including those affecting consumer rights. While promising, these proposals also highlight the limitations of existing laws and the urgent need for harmonization, enforcement mechanisms, and the development of standards that prioritize human oversight, explainability, and non-discrimination.

At the heart of the issue lies a legal paradox: while AI technologies have the potential to enhance efficiency, personalization, and access in consumer markets, they also

threaten to destabilize core legal protections that have long ensured the equitable treatment of individuals. The law, therefore, is confronted with a dual imperative, to facilitate innovation and economic growth, while upholding the rights and dignity of the consumer in an increasingly automated environment. This tension underscores the need for a renewed legal discourse capable of reconciling technological advancement with the foundational values of fairness, transparency, and accountability that underpin consumer law.

2. Legal implications of automated consumer decisions

As artificial intelligence becomes embedded in consumer markets, one of the central legal questions is whether existing consumer protection laws are capable of responding to the risks posed by algorithmic decision-making. Traditional consumer law has developed around the premise of human-led commercial practices, assuming identifiable decision-makers and observable conduct. AI disrupts these assumptions by introducing automated, data-driven systems that often operate without direct human intervention and whose internal logic is frequently inaccessible to both consumers and regulators.

In the European context, the Unfair Commercial Practices Directive (2005/29/EC) provides a general framework designed to protect consumers against misleading and aggressive business practices. However, its application to algorithmically personalized practices, such as dynamic pricing or targeted advertising, remains ambiguous. While some scholars argue that algorithmic manipulation could fall under the prohibition of "misleading actions" or "omissions," enforcement challenges persist due to the technical opacity of AI systems and the difficulty of proving consumer detriment in individualized decision-making contexts (Calo, 2013; Helberger et al., 2020). This raises questions about the adequacy of general clauses in consumer law to effectively capture the subtleties of AI-driven harms.

A key principle in consumer law is transparency, the idea that consumers should be clearly informed about the nature of transactions and the basis for decisions affecting them. Yet algorithmic systems routinely violate this principle. Many AI applications are designed as "black boxes," meaning their inputs and decision-making processes are not easily understandable, even to their developers. This lack of explainability undermines consumers' ability to understand why a particular outcome (such as a higher insurance premium or a denied loan) has occurred, thereby frustrating their ability to make informed decisions or contest unfair outcomes (Wachter et al., 2017).

Closely tied to transparency is the principle of accountability, which requires identifying who is responsible when things go wrong. Traditional legal doctrines, such as liability for breach of contract or tort, depend on tracing causation and attributing responsibility. However, AI systems often operate autonomously and adaptively, complicating efforts to assign legal accountability. The diffusion of responsibility among AI developers, data providers, and service operators further obscures legal liability. Scholars such as Yeung (2018) and Ebers (2021) have emphasized that this "accountability gap" is a structural weakness in the current legal response to AI technologies.

Another pressing concern is the inadequacy of redress mechanisms for consumers adversely affected by automated decisions. Effective redress requires that consumers are aware of the decision, understand it, and have the ability to challenge or appeal it. In practice, most consumers lack both the technical literacy and the procedural avenues to dispute algorithmic outcomes. Automated decisions are often made in real-time, and

platforms rarely offer meaningful explanations or accessible appeals processes. While legal frameworks in some jurisdictions include general rights to complain or seek compensation, these mechanisms tend to be underdeveloped or procedurally burdensome in the context of AI, creating a practical denial of justice for many affected individuals (Zarsky, 2016).

These deficiencies have prompted increasing debate about whether new regulatory instruments are needed to supplement or reform existing consumer protection regimes. Proposals for dedicated AI legislation, such as the EU Artificial Intelligence Act, reflect the growing consensus that conventional consumer law is not fully equipped to safeguard individuals against the systemic risks posed by automated decision-making. Without stronger requirements for transparency, human oversight, and accessible remedies, consumers will remain in a disadvantaged position, subject to decisions that may be efficient from a business perspective but fundamentally unfair from a legal and ethical standpoint.

The intersection of artificial intelligence with personal data processing renders data protection law central to the governance of automated decision-making. In Europe, the General Data Protection Regulation (GDPR) is the most advanced and comprehensive legal framework for data processing, offering robust individual rights and setting strict conditions for the use of personal data in algorithmic systems. However, the emergence of AI technologies has exposed significant tensions between the regulation's foundational principles and the technical realities of machine learning.

One of the most contentious provisions is Article 22 GDPR, which provides individuals with the right not to be subject to decisions based solely on automated processing, including profiling, that produce legal or similarly significant effects. This right embodies the broader data protection goals of human dignity, autonomy, and informational self-determination. Yet the practical reach of Article 22 has been subject to divergent interpretations in legal scholarship and regulatory guidance. Some argue that its scope is narrow, applying only when decisions are fully automated and have significant consequences, thus excluding many real-world scenarios where minimal human involvement exists (Wachter et al., 2017; Edwards & Veale, 2017).

Compounding the challenge is the ambiguous requirement of a "right to explanation." Although the GDPR emphasizes transparency and fairness (Articles 5, 13, 14), it stops short of mandating a detailed explanation of algorithmic logic in every case. As a result, individuals subjected to AI-driven decisions are often left without meaningful insight into how or why a decision was made. This undermines both the enforcement of data subject rights and the broader objective of promoting accountability, which is one of the GDPR's foundational principles (Article 5(2)). Scholars have consistently highlighted the difficulty of reconciling opaque machine learning models (particularly deep learning algorithms) with GDPR mandates for intelligibility and interpretability (Kaminski, 2021).

On the ground, compliance challenges are pervasive, particularly in sectors such as finance, insurance, and e-commerce where algorithmic profiling is prevalent. Organizations often lack adequate technical mechanisms to provide individualized explanations, assess algorithmic fairness, or ensure compliance-by-design with GDPR requirements. While Data Protection Impact Assessments (DPIAs) under Article 35 offer a tool for preemptively managing risk, their actual implementation in AI contexts remains uneven, and many regulators have noted deficiencies in how these assessments address bias, data quality, or automated logic.

Case law and enforcement actions further reveal the regulatory difficulties in addressing AI-driven harms. A notable example is the French CNIL's action against the government's use of the Parcoursup platform, where algorithmic opacity in university admissions raised concerns about the lack of transparency and insufficient human intervention. Similarly, the Dutch District Court in the SyRI case (2020) ruled against the use of an algorithmic system for detecting welfare fraud, finding it violated the right to privacy under the European Convention on Human Rights due to insufficient transparency and proportionality. These cases mark a judicial recognition that the procedural and substantive guarantees of data protection law must be preserved even in the face of efficiency-oriented technological deployments.

More recently, the European Data Protection Board (EDPB) and national supervisory authorities have issued guidelines addressing AI-specific risks, such as the EDPB's Guidelines on Automated Decision-Making and Profiling (2022). These emphasize the necessity of explainability, fairness, and the proactive assessment of risks throughout the AI lifecycle. However, scholars have noted that enforcement remains reactive and fragmented, with a reliance on individual complaints rather than systemic oversight (Mahieu et al., 2021). This reactive posture often leaves structural harms unaddressed and fails to incentivize meaningful organizational change.

The cumulative effect of these regulatory and judicial developments underscores a central tension: while the GDPR offers a powerful legal infrastructure to safeguard personal data, its mechanisms are not always well-suited to the specific features of modern AI systems. Questions remain as to how effectively regulators can enforce rights in a landscape where decision-making is increasingly distributed, probabilistic, and non-intuitive. As algorithmic decision-making proliferates, ensuring legal compliance will require not only more granular interpretations of existing norms but also the development of operational standards that can translate legal principles into practice, an effort currently underway in regulatory initiatives such as the EU Artificial Intelligence Act, which seeks to complement data protection law with AI-specific safeguards.

3. Ethical challenges

The ethical implications of automated decision-making in consumer markets reach far beyond legal compliance. While legislation such as the GDPR and consumer protection directives offer a baseline of individual rights, they do not fully address the deeper normative tensions introduced by algorithmic systems, particularly those related to fairness, bias, manipulation, and consumer autonomy. Ethical scrutiny, therefore, becomes essential for understanding the broader social impact of AI technologies and for guiding the responsible development of systems that increasingly shape everyday consumer experiences.

One of the most significant ethical challenges is algorithmic bias. Automated systems rely on data (both historical and real-time) to inform decisions. However, data is rarely neutral. It reflects societal inequalities, systemic exclusions, and past discriminatory practices. When this data is used to train algorithms, those biases can be inherited and embedded into the system's logic. In domains such as credit scoring, insurance pricing, or targeted advertising, these biases can disproportionately harm vulnerable or marginalized consumer groups, exacerbating existing inequalities under a veneer of objectivity. Scholars such as Barocas and Selbst (2016) have pointed out that algorithmic discrimination may occur even when sensitive characteristics like race or gender are not explicitly included, due to the proxy effect of correlated variables.

Despite this, the use of AI in consumer decision-making also brings potential ethical benefits. Properly designed and monitored, algorithms can enhance efficiency, reduce human bias, and expand access to services. For example, in credit assessment, automated systems might evaluate applicants using alternative data sources, such as utility or rental payment histories, thereby offering credit opportunities to consumers traditionally excluded from formal financial systems. Such innovations can promote financial inclusion, reduce administrative costs, and enable faster service delivery. However, the ethical value of these benefits depends heavily on the conditions of deployment: without transparency, fairness testing, and human oversight, the same tools may also be used to entrench exclusion or manipulate behavior.

Fairness, a core ethical and legal principle, becomes particularly contentious in algorithmic contexts because it lacks a universally accepted definition. Some models operationalize fairness as equal treatment ensuring that individuals with similar attributes receive similar outcomes, while others emphasize group-based equity or the removal of disparate impact. These models can conflict in practice, and optimizing one form of fairness often compromises another (Binns, 2018). In commercial applications, where optimization objectives are often driven by profit or efficiency, fairness tends to be deprioritized unless external legal or reputational pressures intervene. Without deliberate design choices that prioritize equitable outcomes, algorithmic systems risk replicating the structural unfairness they promise to eliminate.

Beyond issues of bias and fairness lies the more subtle but no less significant concern of consumer autonomy. In traditional consumer protection theory, autonomy is safeguarded through principles such as informed consent, the right to withdraw, and protection from undue influence. Yet in algorithmically curated environments, the capacity of consumers to exercise genuine choice is increasingly undermined. Recommendation engines, behavioral targeting, and dynamic pricing strategies all operate on the basis of probabilistic predictions about consumer preferences, which can result in a form of digital paternalism. Instead of empowering consumers, algorithms may steer them toward pre-determined outcomes designed to maximize engagement or profit, effectively reducing individuals to behavioral data points.

This erosion of autonomy is ethically troubling because it undermines the notion of the rational, self-determining consumer. Studies have shown that consumers are often unaware of how they are being profiled, segmented, or nudged by AI systems (Susser, Roessler, & Nissenbaum, 2019). Even when disclosures are made, they are typically buried in dense privacy policies or framed in technical jargon that fails to support meaningful understanding or informed decision-making. As a result, the ethical ideal of consent becomes largely formalistic, devoid of substantive empowerment.

Moreover, the ethical architecture of many algorithmic systems lacks procedural justice, a principle concerned not only with outcomes but with the fairness and legitimacy of the processes through which decisions are made. Consumers subject to automated decisions are often denied meaningful participation in those processes. They have limited visibility into how algorithms work, few options for recourse, and virtually no role in how such systems are designed or governed. This raises profound ethical concerns about power asymmetries between large digital firms and individual consumers, an imbalance that is further exacerbated by data monopolies, proprietary algorithms, and weak accountability structures.

Despite these challenges, the ethical discourse on AI is not without constructive proposals. Many scholars and institutions advocate for "ethical-by-design" approaches,

which integrate ethical principles such as transparency, accountability, and fairness into the technical development lifecycle of AI systems. Tools such as algorithmic impact assessments, fairness auditing frameworks, and explainability metrics are being developed to operationalize these values. The IEEE's Ethically Aligned Design and the European Commission's Ethics Guidelines for Trustworthy AI are two examples of initiatives aimed at embedding ethics into the AI ecosystem from the ground up. However, the effectiveness of these tools remains contingent on enforcement mechanisms and the willingness of firms to go beyond minimum legal compliance.

Ethical frameworks alone, however, are not sufficient. There is a risk that ethics becomes a rhetorical shield, invoked by companies to signal responsibility without committing to meaningful change. Critics have termed this phenomenon "ethics washing," warning that voluntary ethical codes can be used to preempt or delay regulatory oversight. To avoid this, ethical guidance must be accompanied by legally enforceable standards, robust institutional oversight, and genuine stakeholder engagement that includes not only technologists and ethicists, but also civil society actors, consumer advocates, and affected individuals.

In sum, while AI offers opportunities to enhance the consumer experience and correct certain human limitations, it simultaneously introduces profound ethical risks that demand more than technical fixes or abstract principles. Addressing algorithmic bias, protecting consumer autonomy, and promoting fairness will require a structural shift in how AI systems are designed, deployed, and governed. This means re-centering human dignity and justice in a domain currently dominated by efficiency and optimization logic. Only by doing so can the promise of AI be reconciled with the ethical foundations of a democratic and equitable consumer society.

4. Regulatory and business responses

The rapid integration of artificial intelligence into consumer markets has exposed not only the limitations of existing legal frameworks but also the institutional unpreparedness to address emerging risks. As the technological capacity of AI systems outpaces regulatory evolution, both public authorities and private actors are under mounting pressure to redefine governance models that ensure ethical compliance, legal accountability, and the safeguarding of fundamental consumer rights.

From a regulatory perspective, traditional consumer and data protection laws have proven insufficiently agile in the face of novel risks. This has prompted a wave of legal innovation, most notably within the European Union, where the proposed Artificial Intelligence Act (AIA) seeks to establish the first comprehensive framework for AI regulation. The AIA introduces a risk-based classification system, placing strict obligations on high-risk AI systems, including those used for credit scoring, biometric identification, and other consumer-relevant applications. These obligations include requirements for human oversight, transparency, data quality, and conformity assessments. Importantly, non-compliance with the AIA would result in significant administrative fines, modeled after the enforcement architecture of the GDPR.

However, as Spulbar (2025) emphasizes, even ambitious regulatory instruments such as the AIA face inherent structural and operational challenges. Among these is the difficulty of defining and assessing risk in dynamic technological environments, as well as the risk of regulatory lag in sectors characterized by rapid innovation. Spulbar points out that while the AIA provides a necessary legal architecture for digital markets, it must

be complemented by sector-specific guidelines, institutional capacity-building, and international cooperation to avoid fragmentation and regulatory arbitrage. Furthermore, effective enforcement mechanisms and resource-equipped supervisory authorities are crucial for ensuring that legal safeguards move beyond aspirational language into tangible protections for consumers.

In parallel, national regulators have begun to issue sectoral guidance on AI governance, focusing on areas such as financial services, online platforms, and digital advertising. For instance, the UK's Financial Conduct Authority (FCA) and Germany's Federal Cartel Office have published advisory frameworks emphasizing algorithmic transparency, fairness audits, and internal accountability mechanisms. These efforts mark a shift toward proactive regulatory supervision, moving beyond post hoc enforcement toward ex ante compliance strategies. However, such models remain uneven across jurisdictions and often lack binding authority, relying instead on soft law mechanisms, such as codes of conduct or best practice guidelines.

Against this backdrop, corporate actors play a decisive role in shaping the practical contours of AI governance. Major firms deploying AI systems are not only technological innovators but also de facto regulators, as their design choices effectively determine how legal and ethical principles are operationalized. This raises critical questions about corporate responsibility, particularly in an environment where algorithmic opacity and commercial secrecy are widespread.

In response, a growing number of companies have adopted AI ethics policies, created internal review boards, and implemented algorithmic impact assessments. Some have developed technical tools for fairness testing, explainability, and bias mitigation. However, these measures are often voluntary, unevenly applied, and lack external validation. There is also a risk of "ethics washing," whereby companies present a superficial commitment to responsible AI without changing their underlying incentive structures or decision-making processes.

Spulbar (2025) rightly identifies this accountability gap as one of the defining challenges of AI-driven markets. He argues that a sustainable legal framework must incentivize firms not only to innovate but to institutionalize ethical safeguards, including independent audits, stakeholder engagement, and transparent reporting. In this context, hybrid regulatory models (combining state oversight with private self-regulation under public scrutiny) are emerging as a viable approach. These models can harness the technical expertise of the private sector while ensuring that consumer protection, fairness, and non-discrimination remain non-negotiable standards.

A notable challenge in aligning regulatory and corporate responses is the lack of interoperable standards and shared metrics. While tools such as algorithmic audits, model cards, and fairness benchmarks exist, there is little consensus on their methodology or reliability. This fragmentation hinders comparability, accountability, and enforcement. International initiatives, such as the OECD's AI Principles or UNESCO's Recommendation on the Ethics of AI, offer a normative foundation, but they are non-binding and lack implementation mechanisms. Spulbar (2025) suggests that standardization at the EU and global level, accompanied by institutional cooperation and cross-border data governance, will be critical to creating a coherent AI market that respects both innovation and human rights.

5. Conculsion

As artificial intelligence continues to transform consumer markets, the traditional legal and ethical foundations of consumer protection face a profound reckoning. Automated decision-making, once a peripheral technological capability, now plays a central role in determining who gains access to credit, how prices are tailored, which products are recommended, and even how risks are assessed. While these developments offer operational efficiencies and commercial advantages, they also introduce new vulnerabilities that challenge long-standing legal norms and moral expectations.

A central conclusion emerging from this analysis is that existing consumer protection frameworks are under strain. Designed for human-centered transactions, these regimes often lack the conceptual and procedural tools to address the systemic opacity, complexity, and scale of algorithmic systems. Rights such as transparency, fairness, and redress (pillars of consumer protection) are increasingly difficult to enforce when decision-making processes are automated, non-intuitive, and shielded by proprietary designs. The very notion of informed consent, once a cornerstone of consumer autonomy, becomes tenuous in the context of predictive analytics and behavioral targeting.

Similarly, the GDPR, while robust in principle, encounters limitations in practice. Provisions such as Article 22 offer protections against fully automated decisions but are narrowly construed, and enforcement mechanisms often depend on individual initiative. The complexity of AI systems further complicates compliance, especially when explainability and accountability cannot be meaningfully achieved without specialized technical knowledge or institutional support. As demonstrated through case law and regulatory developments, the need for clearer, enforceable standards is no longer a theoretical concern but a practical necessity.

On the ethical front, algorithmic bias and the erosion of consumer autonomy stand out as pressing concerns. The potential for AI to replicate or intensify social inequalities through biased data or opaque logic is well-documented. Likewise, the commodification of consumer behavior, where users are continuously profiled, segmented, and steered, raises questions about manipulation and dignity. While ethical guidelines and design principles exist, they often lack enforceability and can be used strategically to resist stricter regulation, a practice increasingly critiqued as ethics washing.

Nevertheless, it would be reductive to frame AI exclusively as a threat. When carefully regulated and ethically designed, AI can support goals such as financial inclusion, access to services, and consumer empowerment. The challenge lies in ensuring that these benefits do not come at the cost of fundamental rights. This requires a recalibration of both regulatory ambition and corporate responsibility.

Emerging legal instruments like the EU Artificial Intelligence Act represent important steps toward this recalibration. By introducing risk-based classifications and technical obligations, such frameworks begin to adapt law to technological realities. However, as Spulbar (2025) rightly argues, legal frameworks must go beyond formal rule-making. They must be complemented by effective enforcement, sectoral specificity, cross-border cooperation, and the standardization of compliance practices. Regulatory innovation, in other words, must be matched by regulatory capacity.

Corporate actors, meanwhile, must internalize the ethical and legal consequences of the systems they deploy. Voluntary governance, though welcome, cannot substitute for binding obligations and external oversight. Firms that operationalize transparency, fairness, and human-centric design are not only more likely to comply with future regulations, they are also better positioned to earn consumer trust in an increasingly skeptical digital economy.

Ultimately, the integration of AI into consumer decision-making marks a pivotal moment for the legal and ethical ordering of markets. The path forward cannot rely on fragmented or outdated doctrines, nor can it defer to technological determinism. Instead, it demands a new social contract, one that aligns innovation with justice, efficiency with accountability, and data-driven progress with human dignity. Only through coordinated efforts among lawmakers, regulators, businesses, and civil society can the promise of AI be reconciled with the rights and values of those it aims to serve.

References:

Barocas, S., & Selbst, A. D. (2016). Big Data's Disparate Impact. California Law Review, 104(3), 671–732.

Binns, R. (2018). Fairness in Machine Learning: Lessons from Political Philosophy. Proceedings of the 2018 Conference on Fairness, Accountability and Transparency, 149–159.

Calo, R. (2013). Digital Market Manipulation. The George Washington Law Review, 82(4), 995–1051.

Ebers, M. (2021). Liability for artificial intelligence and EU consumer law. J. Intell. Prop. Info. Tech. & Elec. Com. L., 12, 204.

Edwards, L., & Veale, M. (2017). Slave to the Algorithm? Why a Right to an Explanation Is Probably Not the Remedy You Are Looking For. Duke Law & Technology Review, 16(1), 18–84.

Helberger, N., Pierson, J., & Poell, T. (2020). Governing online platforms: From contested to cooperative responsibility. The Information Society, 36(1), 1–14.

Kaminski, M. E. (2021). The right to explanation, explained. In Research handbook on information law and governance (pp. 278-299). Edward Elgar Publishing.

Mahieu, R., Asghari, H., Parsons, C., van Hoboken, J., Crete-Nishihata, M., Hilts, A., & Anstis, S. (2021). Measuring the Brussels effect through access requests: Has the European general data protection regulation influenced the data protection rights of Canadian citizens?. Journal of Information Policy, 11, 301-349.

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

Susser, D., Roessler, B., & Nissenbaum, H. (2019). Online Manipulation: Hidden Influences in a Digital World. Georgetown Law Technology Review, 4(1), 1–45.

Wachter, S., Mittelstadt, B., & Floridi, L. (2017). Why a right to explanation of automated decision-making does not exist in the General Data Protection Regulation. International Data Privacy Law, 7(2), 76–99.

Yeung, K. (2018). Algorithmic Regulation: A Critical Interrogation. Regulation & Governance, 12(4), 505–523.

Zarsky, T. (2016). The Trouble with Algorithmic Decisions: An Analytic Road Map to Examine Efficiency and Fairness in Automated and Opaque Decision Making. Science, Technology, & Human Values, 41(1), 118–132.

*** - SyRI Case (Rechtbank Den Haag 5 February 2020, ECLI:NL:RBDHA:2020:865). - https://uitspraken.rechtspraak.nl/details?id=ECLI:NL:RBDHA:2020:1878

*** - European Data Protection Board (EDPB), Guidelines 05/2020 on consent under Regulation 2016/679 (Version 1.1), May 2020. - https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_en.pdf

*** - CNIL (2018). Deliberation n° 2018-327 on the Parcoursup algorithm. -

https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000037559521
*** - IEEE. (2019). Ethically Aligned Design: A Vision for Prioritizing Human Well-being with Autonomous and Intelligent Systems, 1st Edition. - https://standards.ieee.org/wp-content/uploads/import/documents/other/ead_v2.pdf
*** - European Commission. (2019). Ethics Guidelines for Trustworthy AI. - https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai

Article Info

Received: July 12 2025
Accepted: August 15 2025

How to cite this article:
Calotă, A.M. (2025). The impact of automated decisions on consumers. Legal and ethical challenges in the AI era. *Revista de Ştiinţe Politice. Revue des Sciences Politiques,* no. 87, pp. 48-58.