doi: 10.15678/PG.2026.75.1.02

Journal of Public Governance
No. 1(75)/2026
ISSN 2956-6061 | e-ISSN 2956-6398

ACCEPTED MANUSCRIPT

Peer-reviewed and accepted for publication. Not yet copyedited, proofread or typeset.

Edyta Szumilas

Material and Procedural Instruments for the Protection of Private Entities Against Public Security Authorities in an Era of Digitisation and Automation of Administrative Decision-Making

Abstract:

Objective: This article examines legal safeguards protecting private entities against public security authorities increasingly relying on digital technologies and automated decision-making systems.

Research Design & Methods: The analysis drew on doctrinal legal research and a review of EU legal instruments, including the GDPR, the Law Enforcement Directive, the AI Act, and relevant constitutional standards.

Findings: Automated decision-making in public security governance increases the risk of unlawful, disproportionate, and non-transparent interference with individual rights. Effective protection requires compliance with legality, necessity, proportionality, and accountability principles.

Implications/Recommendations: Regulatory frameworks should strengthen transparency obligations, human oversight, algorithmic auditing, and access to effective remedies.

Contribution/Value Added: The article proposes a three-layer model of protection combining substantive legal safeguards, procedural guarantees, and institutional oversight mechanisms to preserve the rule of law in digital administration.

Article classification: theoretical article

Keywords: automated decision-making; digital governance; public security; administrative law; transparency; private entities

JEL classification: K23, K24, K40

About this version: This is the accepted manuscript of an article peer-reviewed and accepted for publication in the Journal of Public Governance. It may differ from the final version of record in language, formatting and pagination. The version of record will replace it on the journal website; the DOI will remain unchanged.

Edyta Szumilas* – PhD Candidate, Doctoral School - Kracow University of Economics, ul. Rakowicka 27, 31-510 Kraków, Poland; e-mail: 1002152@student.uek.krakow.pl; ORCID: 0000-0002-0493-408

1. Introduction

Public administrations are increasingly deploying algorithmic systems to assist or make decisions in security-sensitive domains - from border control and policing to emergency management. Automated decision-making (ADM) promises efficiency and large-scale data analysis, but raises profound rule-of-law concerns. When a public-security algorithm classifies individuals or firms as risks or issues security measures, the affected parties may face significant legal and practical consequences. The tension between security and liberty is not new, but digital automation deepens it: opaque software may evade conventional checks and make it harder to enforce due process. Integrating automated decision-making into public law has the potential to improve quality and efficiency, but equally it can influence the realization of key procedural values of public law (Hofmann, 2024). The following research question arises: What substantive and procedural safeguards protect private entities when public security authorities rely on digitized and automated administrative decision-making? In order to address this question, the existing legal framework is examined and a layered model of legal protection is developed. The first layer comprises substantive legal safeguards, including clear statutory bases for data processing and constitutional limitations grounded in the principles of legality, proportionality, and privacy protection. The second layer is procedural: transparency, the right to explanation and contestation, human oversight, and effective remedies. The third layer is institutional: auditing, logging, independent oversight and liability of authorities.

This study focuses on public security contexts because they intensify legal tensions. Security agencies often operate under urgency and secrecy, justifying broad powers that may bypass normal procedural safeguards. Embedding algorithms in this setting risks normalized surveillance or discrimination without notice. We therefore scrutinize how EU law and human rights principles apply to ADM in security.

The article is structured as follows. The first section outlines the research methodology and explains the analytical approach adopted in the study. The second section presents a review of the literature on digital governance, automated decision-making, and public security. The main part of the article examines the material and procedural safeguards available to private entities affected by automated decisions made by public security authorities. Particular attention is given to the principles of legality, proportionality, transparency, explainability, human oversight, and access to legal remedies. The analysis is subsequently expanded to include institutional mechanisms designed to ensure accountability and effective su-

pervision of automated systems. The final section summarizes the main findings, discusses the limitations of the study, and identifies directions for future research.

2. Materials and Methods

The study is based on the doctrinal legal research method. An analysis was conducted of primary legal sources, including statutes, international treaties, and judicial decisions, as well as European Union policy documents and relevant academic literature. Particular attention was given to the Charter of Fundamental Rights of the European Union, Regulation (EU) 2016/679 (GDPR), Directive (EU) 2016/680 on data protection in law enforcement, Regulation (EU) 2024/1689 (AI Act), related legislative initiatives concerning artificial intelligence, and selected national legal acts governing public security, including Polish legislation. Literature was selected on the basis of relevance to algorithmic governance, public administration, ADM and AI regulation within EU law.

The research adopts a comparative and analytical perspective. The analysis was conducted in three stages. First, legal safeguards applicable to automated decision-making were identified and systematized, including both substantive legal limitations and procedural guarantees. Next, their operation in the field of public security was examined. Finally, the existing legal framework was evaluated in light of core rule-of-law principles, such as legal certainty, reviewability of decisions, and the accountability of public authorities.

The study proceeds from the hypothesis that traditional safeguards derived from administrative law remain relevant in the context of automated security decision-making but are insufficient on their own to ensure effective protection of individuals. Their effectiveness depends on the incorporation of additional digital governance mechanisms specifically designed for AI-driven and data-intensive systems. In particular, the mere requirement of "human oversight," unless accompanied by clear legal standards regarding its scope, content, and implementation, is unlikely to provide meaningful protection against the risks associated with advanced automated security technologies.

3. Literature Review

The literature on algorithmic governance and public administration has expanded substantially over the past decade. One important strand of scholarship highlights the potential benefits of automated decision-making systems in the public sector. From this perspective, automation is often associated with greater efficiency, more consistent administrative decisions, and improved capacity for real-time risk assessment. In a related vein, algorithmic

regulation is understood as a governance model grounded in the continuous collection and analysis of data for the purpose of managing risks and shaping behaviour (Yeung, 2018).

Building on this broader account of algorithmic governance, Novelli, Taddeo, and Floridi argue that artificial intelligence is becoming an increasingly important component of contemporary public administration, but that its deployment cannot be evaluated solely in terms of administrative efficiency. In their view, AI systems operate within complex socio-technical environments and therefore require robust mechanisms of accountability, oversight, and institutional control. From a governance perspective, the effective integration of AI into public administration depends on regulatory and organisational frameworks capable of ensuring transparency, risk assessment, legal compliance, and the protection of fundamental rights. They further emphasise that public institutions must retain the capacity to monitor, audit, and contest algorithmically supported decisions if democratic legitimacy and public trust are to be preserved. AI governance is thus presented not as a purely technical challenge, but as a broader institutional process aimed at balancing technological innovation with accountability, ethical principles, and the public interest. (Novelli, Taddeo & Floridi, 2023).

At the same time, the growing deployment of automated decision-making systems across a wide range of policy domains is reshaping administrative processes and the implementation of public policies, making automation an increasingly significant feature of contemporary public governance (Hofmann, 2024). However, this development has also prompted concerns about the opacity of algorithmic systems, their limited transparency and accountability, and the concentration of decision-making power within complex technical infrastructures that remain largely inaccessible to meaningful public scrutiny. Scholars have argued that these conditions may also facilitate the reproduction and amplification of existing social inequalities and biases (Pasquale, 2015; Citron, 2008). Contemporary forms of algorithmic regulation increasingly rely on continuous monitoring, behavioural prediction, and pre-emptive intervention, thereby extending regulatory influence beyond traditional mechanisms of legal enforcement (Yeung, 2018).

In this context, accountability has emerged as a central issue in the governance of artificial intelligence. The literature stresses that effective accountability mechanisms are essential for ensuring transparency, assigning responsibility for algorithmic outcomes, and sustaining public trust in AI-enabled decision-making processes (Floridi et al., 2018; Citron & Pasquale, 2014). Relatedly, explanations of automated decisions have been shown to offer only limited protection for affected individuals unless they are accompanied by meaningful

procedural safeguards, opportunities for contestation, and mechanisms for human review. Explanations, in a broader sense, do not necessarily require the general public to obtain a comprehensive understanding of how algorithmic systems function. While such interpretability is clearly desirable and should be encouraged, explanations can in principle be provided without fully opening the mechanism of the system. If explanations are understood primarily as tools that enable affected individuals to act, rather than merely to understand, then their scope and content should be assessed in relation to the specific purposes or actions they are intended to support. (Wachter et. al., 2018).

A similar balance between promise and limitation appears in scholarship that focuses on rule of law values. Automation is increasingly viewed as a means of improving governmental decision-making by enhancing efficiency, reducing costs, and supporting transparency, accountability, consistency, and predictability. Yet the literature also shows that these benefits are not always realised in practice, often because of design and implementation failures rooted in human decisions made at the development stage. Although some highly structured systems demonstrate that automation can be compatible with legal and ethical standards, many machine learning applications raise concerns about opacity, accountability, and bias. These concerns are especially significant in high-impact decisions affecting individual rights, where reliance on proprietary or technically complex algorithms may undermine procedural fairness. As systems become more sophisticated, there is also a growing risk that decision-making becomes unintelligible to non-experts, weakening democratic oversight and diffusing responsibility. For this reason, the literature continues to emphasise the importance of human oversight and context-sensitive evaluation of automation if rule of law principles are to be respected, even though translating those principles into technical systems remains a substantial challenge. (Zalnieriute et al., 2019).

A further body of work moves the discussion from governance and accountability to the more specific question of fairness in machine learning. Current research on fair machine learning largely focuses on technical interventions at the stages of data processing, model training, and post-processing. While this approach reflects the typical responsibilities of data scientists, it also risks reducing fairness to a narrow set of predefined protected attributes derived from legal frameworks. Such a reduction may overlook the broader normative foundations of fairness, as well as the contextual reasons why certain characteristics are protected in the first place. Drawing on philosophical theories of justice, scholars argue that algorithmic fairness cannot be fully captured through static categories alone, since meaningful assessments often depend on contextual factors that are not available in standard datasets.

These may include individual responsibility, social circumstances, and broader life context. As a result, there is increasing recognition that purely data-driven approaches to fairness are limited, and that more context-sensitive and theoretically informed frameworks are needed to address discrimination and justice in machine learning systems adequately. (Binns, 2018).

This debate is also particularly visible in European legal scholarship, where AI systems are seen as tools that may improve efficiency and consistency in public administration, but at the same time raise concerns regarding core principles of administrative law, including legality, transparency, accountability, and due process, especially in high-risk areas such as welfare, policing, and migration control. The AI Act is therefore presented as an important first step in addressing these challenges through transparency obligations, risk assessments, and requirements for human oversight. Nevertheless, the literature points to significant limitations, including the vague definition of "meaningful human oversight," the limited scope of procedural rights for individuals, and the insufficient mechanisms available to challenge automated decisions. Overall, scholars argue that the effectiveness of the framework will depend on national implementation and on stronger integration with administrative and judicial safeguards to ensure that algorithmic governance remains consistent with fundamental rights and the rule of law (Pavlidis & Kastanas, 2026).

Domestic legal scholarship advances a similar concern. Some authors argue that existing procedural frameworks have not yet been sufficiently adapted to the automated handling of cases by public administrative authorities, which may create risks for the protection of individual rights. On this view, the automation of administrative functions requires further legislative development, including the establishment of clear legal bases for automation, the updating of procedural rules, and the introduction of adequate safeguards for procedural rights. These safeguards should include, in particular, the right to meaningful human intervention and the right to be heard, or to present one's position (Geburczyk, 2021).

Empirical research adds an important corrective to the more normative strands of the literature. Findings from a study conducted among respondents in one Polish city, cited by Chmura-Szczecińska (2021), indicate differentiated attitudes towards the acceptability of automation in legal decision-making. Acceptance depends on the nature of the case: it is lower in matters requiring contextual judgment, considerations of fairness, and attention to individual circumstances, such as family or criminal cases, while it is higher in cases characterised by simple and standardised factual patterns, especially in selected administrative or civil proceedings. Respondents also relatively often support arrangements in which automated decisions are subject to human approval or are triggered only with the consent of

the party concerned, although concerns are raised about the substantive value of such oversight when it is merely formal. Alternatively, emphasis is placed on effective appeal mechanisms that would allow algorithmic decisions to be reviewed without requiring ex ante human intervention in every case. Overall, these findings suggest that, although automation in legal decision-making is perceived as a means of increasing procedural efficiency, its social and legal acceptability remains dependent on adequate procedural safeguards and the continued central role of human actors within decision-making systems (Chmura-Szczecińska, 2021; Waldman & Martin, 2022).

Taken together, the literature presents algorithmic governance as a field defined by a persistent tension between efficiency and legality, innovation and accountability, and automation and human judgment. While the potential of AI to improve administrative performance is widely recognised, the dominant scholarly position remains cautious: automation may support public administration, but only if it is embedded in robust legal, institutional, and procedural safeguards.

4. Results Discussion

A coherent rule-of-law framework for state-sponsored ADM must begin with a clear legal foundation. Under the EU Charter, any restriction of fundamental rights must be "provided for by law" and respect the essence of the right (CFREU, Article 52). In practice this means that governments cannot deploy new surveillance powers by executive whim: any police or border algorithm must be grounded in statute or duly promulgated regulation that clearly defines its scope. The CJEU has repeatedly emphasized that powers affecting rights must be precisely defined (see Case *9/56, Meroni & Co., Industrie Metallurgiche, SpA v High Authority EU:C:1958:7).* Many Member States have security laws, but few explicitly mention digital profiling; legislators should amend these laws to cover ADM explicitly, ensuring notice and accountability. Even with a legal basis, substantive limitations like proportionality and necessity must be respected. Any automated measure must genuinely advance a legitimate public-security objective and be the least intrusive means available. It is not enough that an algorithm could identify a threat; it must be shown that its use is truly necessary for public safety. In legal terms, the EU requires that data processing be "adequate, relevant and limited to what is necessary" (GDPR, Article 5(1)(c)). Similarly, the AI Act imposes risk-management obligations on high-risk AI: providers must ensure that training and test datasets are representative, accurate and free of bias, and that error rates are minimized (AI Act, Articles 9-10). In short, proportionality requires trimming any excess collec-

tion or uses of data, and rigorous testing of any automated system to show it actually improves security rather than casting an overly wide net. Equally crucial are rights-based limits, especially privacy and anti-discrimination. Many security AIs process sensitive personal data: biometrics, health, ethnic or religious information. Such "special-category" data are prohibited from profiling under GDPR Article 9 unless strict conditions are met. Even then, any intrusion must be narrowly tailored and accompanied by safeguards. Moreover, EU equality law forbids systematic targeting of protected groups. The Charter's Article 21 flatly prohibits "any discrimination" on grounds such as race, ethnicity, gender or religion. An infamous example is the Dutch "child benefits" scandal: a welfare-fraud algorithm explicitly included nationality as a risk factor. Non-Dutch parents were flagged almost exclusively, creating a "discriminatory loop" of profiling. This scheme, though justified as risk-based violated basic equality and proportionality principles (ESPN *Flash Report, 2021*). EU courts and parliaments must prevent analogous outcomes by banning algorithmic filters that correlate with ethnicity or other protected traits, even indirectly. Equally important is transparency of legal authorization. Not only must the algorithms be lawful, but the enabling laws themselves must be accessible and precise. Blanket emergency powers undermine legal certainty. This aligns with the Charter's foreseeability principle under Article 52(1) and the GDPR's insistence that processing have a clear legal basis. Beyond formal legality, administrative law demands notice: Article 41(2)(a) of the Charter guarantees the right to be heard before any adverse measure is taken. In practical terms, even before an algorithm touches an individual, that person should at least have access to the general rules or criteria used. On the procedural side, affected persons must receive notice and explanation for algorithmic decisions. GDPR Articles 13–15 already provide that data subjects are entitled to know if automated profiling affects them and to get "meaningful information about the logic involved". By analogy, a person flagged by a police AI or denied a benefit by a social-services algorithm should be informed (even if indirectly) that a machine-assisted decision was made. Full transparency may conflict with law enforcement secrecy, but some disclosure is required. Even after the fact, authorities should be prepared to explain how a decision was reached in general terms: which data categories were considered, what risk factors were weighted, and what impact the outcome has (OECD, *Procedural Fairness and Transparency: Key Findings*, 2012). GDPR Art.22(3) and the Law Enforcement Directive Art.11 provide that fully automated decisions producing legal effects are prohibited unless the individual has the right to human intervention, to state their case and to contest the decision. The adoption of the AI Act adds an additional regulatory layer to the governance of automated

decision-making in the public sector. By introducing a risk-based framework, the Regulation imposes specific obligations on providers and deployers of high-risk AI systems, including requirements relating to risk management, documentation, data governance, human oversight, and post-market monitoring. Although the AI Act does not establish a comprehensive procedural regime for administrative decision-making, it strengthens existing safeguards by promoting transparency, accountability, and reviewability of algorithmic systems. In public security contexts, these obligations may contribute to reducing the risks associated with opacity, bias, and excessive reliance on automated outputs. The effectiveness of these mechanisms, however, will depend largely on their practical implementation and their interaction with existing guarantees derived from administrative law, data protection law, and fundamental rights standards. The AI Act similarly mandates that high-risk systems be designed with human supervisors in mind. However, the mere presence of a human in the loop is insufficient. People tend to unquestioningly follow algorithmic suggestions if they know a machine produced them. For example, UK police using the HART recidivism tool in Durham were supposed to be free to reject its risk scores, but in practice officers almost always acted on the algorithm's recommendation. In effect they turned a decision-support tool into a de facto automated decider (Oswald & Grace, 2018). To make oversight real, the human must have true discretion and competence. This means: training operators to understand and critically assess the tool's output, giving them authority to override or modify it without penalty, requiring documentation of their reasoning.

Linked to oversight is the classic right to be heard and to adversarial process. Administrative procedure law traditionally gives people the opportunity to respond before a final decision. In the automated setting, this should be preserved. Procedural fairness demands that those targeted by ADM have their say. Above all, there must be judicial review and effective remedies. The Charter (Article 47) guarantees "effective remedy and fair trial" for any violation of EU law, and Article 41(2)(c) obliges authorities to "give reasons" for their decisions. One cannot meaningfully appeal an automated denial if one does not understand the reasons. Thus courts must have the power to examine algorithm-based decisions. In practice, judges should be able to review the code or data of an algorithm if a person complains. This might require special procedures: for instance, national laws could allow intelligence or labor courts to see classified algorithms in camera or appoint vetted special advocates. At minimum, if source-code disclosure is impossible, authorities should be forced to articulate an ex post "substitute reasoning" - a logical explanation that justifies the outcome without revealing secrets. Remedies should include not just quashing wrongful decisions but

also damages: EU law (Article 340 TFEU/Charter Article 41(3)) and member-state law generally provide that victims of unlawful acts by public authorities can be compensated. Agencies must remain liable even if an algorithm was used.

Building on these principles requires robust institutional safeguards. First, every ADM deployment needs logging and auditing. Just as controllers must keep processing records under GDPR Art.30, agencies should automatically log every algorithmic decision: inputs, model version, output and final human action taken. These logs should be audited regularly by independent bodies and made available in anonymized form to affected individuals on request. Second, independent oversight bodies must be empowered. Data protection authorities already oversee law-enforcement data use and should be tasked to audit algorithms in policing, immigration and other areas. Third, accountability and liability must be clear. If a public algorithm causes wrongful harm, officials must face consequences. An algorithm is no excuse to shirk liability. In practice, courts should treat an agency and its officers as fully responsible for decisions made with algorithmic support.

The author argues that the foregoing analysis demonstrates the need for a multi-layered approach to the governance of automated decision-making in public security contexts. The diversity of ADM systems and the range of legal, technical, and institutional risks they generate make it difficult to address these challenges through any single category of safeguards. Substantive legal limitations, procedural guarantees, technical governance measures, and institutional oversight mechanisms should therefore be regarded as complementary and mutually reinforcing elements of an effective framework of protection.

The author further argues that the increasing use of automated systems in public administration is both difficult to avoid and capable of generating significant public benefits. ADM systems may enhance administrative efficiency, improve consistency in decision-making, and facilitate the processing of large volumes of information. At the same time, their deployment creates risks related to opacity, discriminatory outcomes, and excessive reliance on algorithmic outputs. For this reason, technological innovation should be accompanied by safeguards capable of ensuring compliance with fundamental rights and rule-of-law requirements.

5. Conclusions

In conclusion, a framework combining substantive legal safeguards, procedural guarantees, and institutional oversight is both normatively justified and practically necessary for the governance of automated decision-making in public security contexts. The pursuit of

security objectives does not displace the fundamental requirements of the rule of law. Principles such as legality, necessity, proportionality, transparency, and accountability continue to apply regardless of whether public authority is exercised directly by human decision-makers or through algorithmic systems.

The analysis has identified persistent regulatory and institutional challenges. Existing legal protections remain unevenly implemented, particularly in the public sector, while the effectiveness of recently adopted regulatory instruments will depend largely on their interpretation and enforcement within national legal systems. The findings confirm the initial hypothesis that traditional administrative-law safeguards remain necessary but are insufficient without additional mechanisms tailored to AI-driven decision-making.

The governance of algorithmic systems cannot be understood as a one-time regulatory exercise. The evolving nature of digital technologies requires continuous review, evaluation, and adaptation. Accordingly, more dynamic forms of oversight are needed, including algorithmic impact assessments, independent audits, external scrutiny of high-risk systems, and enhanced institutional capacities for monitoring automated decision-making. Such mechanisms may help operationalise fundamental rights and rule-of-law principles in increasingly complex technological environments.

Existing EU legal frameworks already incorporate important safeguards, including restrictions on fully automated decision-making, rights associated with good administration, and requirements for human oversight in high-risk AI systems. Nevertheless, significant uncertainties remain regarding their practical effectiveness, particularly where secrecy, efficiency, or national security concerns limit transparency and accountability. Future research should therefore focus on empirical assessments of algorithmic decision-making in areas such as policing, border management, and migration control, as well as comparative evaluations of different regulatory approaches.

Ultimately, the deployment of AI in public governance does not eliminate the requirements of the rule of law but instead requires their adaptation to digital decision-making environments. The long-term legitimacy of algorithmic governance will depend on whether automated systems remain subject to legal constraints, procedural fairness, transparency, and effective accountability.

Finally, the author argues that the challenges associated with ADM cannot be understood solely as a consequence of technological novelty. While public administrations have historically adapted legal and institutional frameworks to technological change, contemporary

ADM systems raise distinct concerns because they increasingly influence the formation, prioritisation, and justification of administrative decisions. As a result, the exercise of public authority may become dependent on processes that are more difficult to scrutinise, review, and contest. This development reinforces the need for effective legal safeguards and institutional mechanisms capable of maintaining transparency and procedural fairness in digitally mediated forms of governance

.

References

Berends, S. (2021). *Dutch child benefit scandal: Origin and latest developments*. ESPN Flash Report 2021/51. European Commission, European Social Policy Network. https://ec.europa.eu/social/BlobServlet?docId=24723&langId=en

Binns, R. (2018). Fairness in machine learning: Lessons from political philosophy. *Proceedings of Machine Learning Research, 81*, 149–159. https://proceedings.mlr.press/v81/binns18a.html

Chmura-Szczecińska, E. (2021). Automatyzacja decyzji w prawie: Pola i granice stosowania [Algorithmic decision making in law: Areas and limits]. *Studia Prawnicze, 2*(224), 135–159. https://czasopisma.inp.pan.pl/index.php/sp/article/view/2730

Citron, D. K. (2008). Technological due process. *Washington University Law Review, 85*(6), 1249–1313.

Citron, D. K., & Pasquale, F. (2014). The scored society: Due process for automated predictions. *Washington Law Review, 89*(1), 1–33.

Court of Justice of the European Communities. (1958). *Meroni & Co., Industrie Metallurgiche, SpA v High Authority*, Case 9/56, ECLI:EU:C:1958:7, [1957–1958] ECR 133.

European Parliament & Council of the European Union. (2016/679). *Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)*. OJ L 119, 4.5.2016, pp. 1–88.

European Parliament & Council of the European Union. (2016680). *Directive (EU) 2016/680 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties*. OJ L 119, 4.5.2016, pp. 89–131.

European Parliament & Council of the European Union. (2024). *Regulation (EU) 2024/1689 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act)*. OJ L, 2024/1689, 12.7.2024.

European Union. (2012). *Charter of Fundamental Rights of the European Union*. OJ C 326, 26.10.2012, pp. 391–407.

European Union. (2016). *Consolidated version of the Treaty on the Functioning of the European Union*. OJ C 202, 7.6.2016, pp. 47–390.

Floridi, L., Cowls, J., Beltrametti, M., Chatila, R., Chazerand, P., Dignum, V., Luetge, C., Madelin, R., Pagallo, U., Rossi, F., Schafer, B., Valcke, P., & Vayena, E. (2018). AI4People: An ethical framework for a good AI society. Opportunities, risks, principles, and recommendations. *Minds and Machines, 28*(4), 689–707. https://doi.org/10.1007/s11023-018-9482-5

Geburczyk, F. (2021). Automatyzacja załatwiania spraw w administracji samorządowej a gwarancje procesowe jednostek: Uwagi de lege ferenda w kontekście ogólnego rozporządzenia o ochronie danych (RODO). *Samorząd Terytorialny, 5*, 21–32.

Hofmann, H. C. H. (2024). Automated decision-making (ADM) in EU public law. In H. C. H. Hofmann & F. Pflücke (Eds.), *Governance of automated decision-making and EU law* (pp. 1–31). Oxford University Press. https://doi.org/10.1093/9780198919575.003.0001

Kastanas, I., & Pavlidis, G. (2025). Algorithmic administration and the EU AI Act: Legal principles for public sector use of AI. *Journal of Ethics and Legal Technologies, 7*(2), 59–79. https://doi.org/10.25430/pupj-JELT-2025-2-3

Novelli, C., Taddeo, M., & Floridi, L. (2024). Accountability in artificial intelligence: What it is and how it works. *AI & Society, 39*(4), 1871–1882. https://doi.org/10.1007/s00146-023-01635-y

OECD. (2012). *Procedural fairness and transparency: Key findings*. OECD Publishing. https://doi.org/10.1787/17f27597-en

Oswald, M., Grace, J., Urwin, S., & Barnes, G. C. (2018). Algorithmic risk assessment policing models: Lessons from the Durham HART model and 'Experimental' proportionality. *Information & Communications Technology Law, 27*(2), 223–250. https://doi.org/10.1080/13600834.2018.1458455

Pasquale, F. (2015). *The black box society: The secret algorithms that control money and information*. Harvard University Press. https://doi.org/10.4159/harvard.9780674736061

Wachter, S., Mittelstadt, B., & Russell, C. (2018). Counterfactual explanations without opening the black box: Automated decisions and the GDPR. *Harvard Journal of Law & Technology, 31*(2), 841–887.

Waldman, A. E., & Martin, K. (2022). Governing algorithmic decisions: The role of decision importance and governance on perceived legitimacy of algorithmic decisions. *Big Data & Society, 9*(1). https://doi.org/10.1177/20539517221100449

Yeung, K. (2018). Algorithmic regulation: A critical interrogation. *Regulation & Governance, 12*(4), 505–523. https://doi.org/10.1111/rego.12158

Zalnieriute, M., Bennett Moses, L., & Williams, G. (2019). The rule of law and automation of government decision-making. *The Modern Law Review, 82*(3), 425–455. https://doi.org/10.1111/1468-2230.12412

Funding
This research received no external funding.
Research Ethics Committee
Not applicable.
Conflicts of Interest
The authors declare no conflicts of interest.
Copyright and License
This article is published under the terms of the Creative Commons Attribution 4.0 License. Published by Małopolska School of Public Administration – Krakow University of Economics, Krakow, Poland.
Data Availability Statement
All data will be available and shared upon request.
AI Declaration Statement
The author used Google Gemini solely for language editing and proofreading purposes. All substantive aspects of the research, including the research design, legal analysis, interpretation of sources, and conclusions, were developed and verified by the author, who assumes full responsibility for the final content of the manuscript.