

The Right to Algorithmic Transparency as a New Constitutional Right: Foundations and Limitations

Mohammed Ali Zaal Al-shabatat

Department of Law,

Applied Science Private University,

Al Arab St. 21, Amman, Jordan

Email: m_alshabatat@asu.edu.jo

<https://orcid.org/0009-0007-5729-6681>

Ziad Alwahshat

Ajloun National University,

Jordan, Ajloun, 26810, Jordan

Email: zyad.wahshat@anu.edu.jo

<https://orcid.org/0000-0002-8550-259X>

Abstract

The rapid expansion of artificial intelligence (AI) and algorithmic decision-making in public administration, private services, employment, finance, justice, and other socially significant fields have created new challenges for contemporary constitutional law. Automated systems increasingly participate in decisions capable of producing legal or similarly significant effects on individuals, while the processes through which those decisions are generated may remain technically complex, institutionally opaque, and difficult to challenge.

This article examines algorithmic transparency as an emerging constitutional right. It argues that such a right should not initially be understood as an absolute or autonomous constitutional entitlement to disclosure of source code or proprietary algorithms. Rather, it should be understood as a constitutional guarantee derived from the interaction of established principles, including the rule of law, equality, non-discrimination, privacy, data protection, procedural fairness, the duty to give reasons, access to information, and effective judicial protection.¹

The article analyzes the conceptual foundations of algorithmic transparency, the transition from traditional administrative transparency to digital and algorithmic transparency, and the technical, legal, ethical, economic, and national-security limitations affecting its implementation. Attention is given to the European Union's General Data Protection Regulation (GDPR) and Artificial Intelligence Act (AI Act), as well as significant judicial developments concerning automated decision-making.² The article also examines the American experience and the emerging Jordanian framework, particularly the Jordanian Constitution, the Right to Access Information framework, and Personal Data Protection Law No. 24 of 2023.

The article concludes that algorithmic transparency should be developed according to a model of relative and proportionate transparency, under which the intensity of transparency corresponds to the degree of risk and the impact of the automated decision on fundamental rights. It proposes five minimum constitutional guarantees: notice of significant automated decision-making, meaningful explanation, human intervention, the right to challenge, and effective independent or judicial review.

Keywords: Algorithmic Transparency; Constitutional Rights; Artificial Intelligence; Automated Decision-Making; Explainable AI; Algorithmic Accountability; Digital Rights; Rule of Law.

I. Introduction

Artificial intelligence has increasingly become part of the institutional infrastructure through which governments, corporations, courts, financial institutions, employers, and service providers make or assist in making decisions. Algorithms can now classify individuals, evaluate risks, rank applications, detect suspected fraud, assess creditworthiness, recommend employment decisions, and support judicial or administrative decision-making. The growing use of these technologies creates substantial opportunities for efficiency, accuracy, and administrative modernization, but it also creates a new form of legal vulnerability: individuals may be subject to decisions whose underlying logic they cannot meaningfully understand or contest.³

The problem is particularly significant where algorithmic systems are used in areas affecting fundamental rights. A person denied a public benefit, classified as a high-risk individual, rejected for credit, subjected to enhanced scrutiny, or adversely assessed by an automated system may face serious consequences without being able to identify the factors that produced the outcome.

Traditional constitutional law developed largely around human decision-makers. Administrative officials could be identified, decisions could be attributed to institutions, reasons could be requested, and judicial review could examine the legality of the exercise of discretion. Algorithmic decision-making complicates this structure because the effective basis of a decision may be distributed among datasets, software, statistical models, machine-learning processes, private vendors, and institutional practices.

The resulting problem is therefore not merely technological. It is fundamentally constitutional.

The central argument of this article is that algorithmic transparency should be regarded as an emerging constitutional right. This does not mean that every constitution already recognizes such a right expressly. Rather, the right may emerge through constitutional interpretation and legislative development from existing guarantees of legality, equality, privacy, procedural fairness, access to information, and judicial protection.

The concept of algorithmic transparency is also distinct from the simple disclosure of source code. A legal requirement that an individual be able to understand and challenge an automated decision does not necessarily require the government or a private entity to reveal every technical detail of a model. The constitutional objective is instead meaningful transparency: information

that enables an affected person, regulator, or court to understand the essential basis of the decision and assess its legality and fairness.⁴

The European Union provides the most developed regulatory example. Article 22 of the GDPR establishes safeguards concerning decisions based solely on automated processing that produce legal effects or similarly significant effects, including, in specified circumstances, rights to human intervention, expression of one's viewpoint, and contestation of the decision.⁵ The EU AI Act subsequently established a broader risk-based framework and requires high-risk AI systems to be sufficiently transparent to enable deployers to interpret their outputs and use them appropriately.⁶

The Jordanian context presents a particularly interesting case. Jordan does not yet possess a comprehensive AI statute comparable to the EU AI Act, but it has constitutional guarantees, an access-to-information framework, and a Personal Data Protection Law enacted in 2023. These instruments provide foundations upon which a more specific framework for algorithmic transparency may be developed.⁷

II. Research Problem

The rapid proliferation of AI and algorithmic decision-making has generated a potential gap between traditional constitutional guarantees and the technological mechanisms through which decisions increasingly occur.

The principal research problem is therefore:

To what extent can algorithmic transparency be recognized as an emerging constitutional right, what constitutional and legal foundations support such recognition, what legitimate limitations restrict it, and how can comparative and Jordanian legal systems operationalize it?

The problem contains several interconnected dimensions.

First, there is a conceptual dimension concerning the meaning of algorithmic transparency.

Second, there is a constitutional dimension concerning whether existing fundamental rights can support recognition of a new digital guarantee.

Third, there is a regulatory dimension concerning the relationship between transparency and privacy, intellectual property, cybersecurity, and national security.

Fourth, there is a judicial dimension concerning the capacity of constitutional and administrative courts to review algorithmic decision-making.

Finally, there is a Jordanian dimension concerning whether existing constitutional and legislative provisions are adequate to protect individuals against opaque automated decisions.

III. Research Questions

This article addresses five principal questions:

1. What is the conceptual and legal meaning of algorithmic transparency?

2. What constitutional principles provide a foundation for recognizing algorithmic transparency as an emerging right?
3. What technical, legal, ethical, and public-interest limitations restrict algorithmic transparency?
4. How have European, American, and Jordanian legal frameworks addressed automated decision-making and algorithmic transparency?
5. What role can constitutional and administrative courts play in developing and operationalizing this emerging right?

IV. Research Hypotheses

The article proceeds from the following hypotheses:

First, algorithmic transparency can emerge as a constitutional right through the digital development of traditional principles such as the rule of law, equality, privacy, due process, access to information, and effective judicial protection.

Second, absolute algorithmic transparency is neither technically feasible nor constitutionally necessary; relative and proportionate transparency provides a more appropriate model.

Third, European regulatory experience provides important mechanisms for balancing algorithmic transparency with privacy, intellectual property, security, and innovation.

Fourth, courts can contribute significantly to the development of algorithmic transparency even where constitutional texts do not expressly refer to algorithms or artificial intelligence.

Fifth, Jordan possesses important constitutional and legislative foundations but requires a more integrated framework governing AI, automated administrative decisions, algorithmic auditing, and judicial review.

V. Research Methodology

The article employs descriptive, analytical, comparative, and critical methodologies.

The descriptive method is used to establish the conceptual meaning of algorithms, automated decision-making, transparency, and explainability.

The analytical method examines constitutional principles, legislation, and judicial decisions to determine the legal foundations and limitations of algorithmic transparency.

The comparative method focuses primarily on the European Union and selected American developments, while treating Jordan as the principal national case study.

The critical method evaluates whether existing legal frameworks are adequate to protect individuals against the risks created by opaque automated decision-making.

The research relies primarily on verified primary sources and established academic literature rather than unverifiable or incomplete references.

VI. The Conceptual Framework of Algorithmic Transparency

A. Algorithms and Automated Decision-Making

An algorithm may generally be understood as a structured set of computational instructions designed to process input and generate output. Contemporary AI systems, however, may operate through machine-learning processes in which the relationship between inputs and outputs is not always readily understandable even to the system's users.

Automated decision-making refers to situations in which a decision is generated wholly or substantially through automated processing, potentially without direct human intervention.

The constitutional significance of such decision-making arises where output affects rights or legally significant interests.

Algorithmic systems are increasingly used in contexts such as credit scoring, employment, insurance, welfare administration, criminal justice, taxation, and policing. Danielle Citron and Frank Pasquale have emphasized that automated scoring can affect access to employment, credit, housing, and insurance while remaining opaque and insufficiently supervised.⁸

The concern is therefore not automation as such. Constitutional concern arises when automated power affects individuals without adequate accountability.

B. The Algorithmic Black Box

The concept of the "black box" describes the difficulty of understanding how an algorithm produces a particular result.

Jenna Burrell identifies three distinct forms of algorithmic opacity: intentional secrecy, lack of technical literacy, and opacity resulting from the complexity and scale of machine-learning systems.⁹

This distinction is particularly important in constitutional analysis.

Corporate secrecy can potentially be addressed through legal disclosure obligations.

Technical illiteracy can be addressed through accessible explanations.

But computational complexity may remain even where there is no intention of concealing information.

Frank Pasquale's analysis of algorithmic secrecy similarly demonstrates how hidden computational systems can exercise substantial social and economic power while remaining difficult for affected individuals to scrutinize.¹⁰

The black-box problem therefore creates a direct relationship between opacity and accountability.

Where individuals cannot understand why a decision occurred, their capacity to challenge it is diminished.

C. Transparency in Constitutional Thought

Transparency is traditionally associated with democratic accountability and the rule of law.

Constitutional transparency may be expressed through:

1. access to information;
2. publicity of governmental action;
3. reason-giving;
4. procedural fairness;
5. judicial review.

Algorithmic systems introduce a new dimension.

Disclosing only the outcome of an automated decision may not constitute meaningful transparency. The affected person may need information about the principal factors that materially influenced the decision.

Kroll and his co-authors argue that traditional accountability mechanisms designed for human decision-makers may be inadequate when decisions are delegated to computational systems.¹¹

Accordingly, the constitutional objective should be to make automated power traceable, reviewable, and contestable.

VII. From Administrative Transparency to Algorithmic Transparency

Traditional administrative transparency was largely concerned with governmental documents, procedures, and decisions.

Digital government has altered this model.

The relevant object of transparency is increasingly not only the administrative decision itself but also the technological infrastructure through which the decision is generated.

The transformation can therefore be represented as:

Administrative Transparency → Digital Transparency → Algorithmic Transparency.

Algorithmic transparency adds at least four elements:

- disclosure that an automated system is being used;
- information concerning the principal factors relevant to the decision;
- explanation sufficient to enable meaningful understanding;
- mechanisms through which the decision can be challenged.

This does not require disclosure of source code in every case.

Indeed, Lilian Edwards and Michael Veale caution that a generalized "right to explanation" should not be treated as a complete solution to algorithmic harms.¹²

The appropriate constitutional approach is therefore not maximum disclosure, but meaningful and proportionate disclosure.

VIII. Algorithmic Transparency as an Emerging Constitutional Right

The central proposition of this article is that algorithmic transparency may be recognized as an emerging constitutional right through the interaction of existing constitutional guarantees.

Its principal foundations are:

1. The Rule of Law

The rule of law requires public power to remain legally accountable.

The use of an algorithm cannot exempt an administrative authority from legal responsibility.

Technological delegation cannot become a delegation of constitutional responsibility.

2. Equality

Algorithmic systems may reproduce discriminatory patterns in training data or through proxy variables.

Transparency allows discriminatory outcomes to be identified and challenged.

Mittelstadt and his co-authors identify bias, discrimination, opacity, privacy, and responsibility as interconnected ethical problems associated with algorithmic systems.¹³

3. Privacy and Data Protection

Individuals cannot effectively exercise control over personal data if they lack meaningful information concerning how those data are processed.

4. Procedural Fairness

A person affected by a significant decision should have an opportunity to understand and challenge the basis of that decision.

5. Duty to Give Reasons

Algorithmic decision-making should not eliminate the traditional legal requirement that significant administrative decisions be adequately reasoned.

6. Effective Judicial Protection

Transparency must ultimately facilitate effective review.

A right that provides information but no mechanism for contesting the resulting decision is incomplete.

IX. The Limits of Algorithmic Transparency

Algorithmic transparency is not absolute.

Its limitations may be divided into four categories.

A. Technical Limitations

Deep-learning systems may involve highly complex statistical relationships.

Even disclosure of the model may not produce a comprehensible explanation.

Explainable AI can mitigate this problem, but post hoc explanations may not always accurately reproduce the internal reasoning of a model.

Wachter, Mittelstadt, and Russell have therefore proposed counterfactual explanations as one possible method of providing useful information without necessarily opening the entire technical "black box."¹⁴

B. Intellectual Property and Trade Secrets

Algorithms may constitute valuable proprietary assets.

A constitutional right to transparency should therefore not automatically require disclosure of source code.

The more appropriate distinction is between:

technical transparency and decision transparency.

The latter may be constitutionally necessary even where the former is protected.

C. Privacy and Third-Party Rights

Transparency may itself create privacy risks.

Disclosure could be exposed:

- personal data;
- information about third parties;
- confidential records;
- sensitive institutional information.

Accordingly, algorithmic transparency should coexist with data minimization and privacy protection.

D. National Security and Public Safety

Certain algorithmic systems may operate in areas involving:

- counterterrorism;
- cybersecurity;

- criminal investigations;
- border security;
- intelligence.

In such circumstances, some restrictions may be legitimate.

However, national security should not function as a blanket of exemption from accountability.

Restrictions should satisfy:

1. legality;
2. legitimate purpose;
3. necessity;
4. proportionality;
5. independent oversight;
6. appropriate remedies.

X. The Principle of Relative Algorithmic Transparency

This article proposes the concept of Relative Algorithmic Transparency as an appropriate constitutional model.

Relative transparency means that the degree of transparency required depends upon the significance and risk of the automated decision.

The EU AI Act itself adopts a risk-based regulatory architecture. Article 13 requires high-risk AI systems to operate with sufficient transparency to allow deployers to interpret outputs and use the systems appropriately.¹⁵

The constitutional significance of this approach is that transparency should become stronger as the potential impact on fundamental rights increases.

XI. The European Experience

A. The GDPR

The GDPR is a central reference point in the development of automated-decision safeguards.

Article 22 provides that individuals have a right not to be subject, in specified circumstances, to decisions based solely on automated processing that produce legal or similarly significant effects. The provision also identifies safeguards including human intervention, the opportunity to express a viewpoint, and the ability to contest the decision in relevant circumstances.¹⁶

The provision is important but should not be overstated.

The GDPR does not create an unrestricted right to obtain the source code of an algorithm.

Nor is there universal agreement that it creates a freestanding, general right to explanation. Wachter, Mittelstadt, and Floridi specifically challenge the proposition that the GDPR creates a general legally enforceable right to explanation.¹⁷

This distinction strengthens rather than weakens the argument of this article.

The constitutional objective should be meaningful explanation and contestability, rather than automatic disclosure of the internal structure of every algorithm.

XII. The EU Artificial Intelligence Act

Regulation (EU) 2024/1689, commonly known as the Artificial Intelligence Act, represents a significant development in European AI governance.

The Regulation was adopted on June 13, 2024, and published in the Official Journal on July 12, 2024.¹⁸

Article 13 requires high-risk AI systems to be designed and developed so that their operation is sufficiently transparent to allow deployers to interpret outputs and use them appropriately.¹⁹

The AI Act therefore moves beyond the narrower data-protection context of the GDPR and establishes a broader risk-based governance framework.

Its significance for constitutional theory lies in the recognition that transparency should be linked to:

- risk;
- human oversight;
- documentation;
- accountability;
- fundamental rights.

XIII. European Judicial Developments

A. The SyRI Judgment

A particularly important judicial development is the SyRI case in the Netherlands.

The District Court of The Hague examined the System Risk Indication (SyRI), an automated system used by the government to identify potential welfare and tax fraud.

The court held that the legal framework governing SyRI violated Article 8 of the European Convention on Human Rights because the interference with private life was insufficiently justified. The court specifically emphasized that the system was insufficiently transparent and verifiable.²⁰

The decision is significant because it demonstrates that algorithmic transparency may become a requirement through existing fundamental rights rather than through a constitutional provision expressly mentioning algorithms.

In other words:

Traditional constitutional rights can constrain technologically new forms of governmental power.

B. SCHUFA and Automated Credit Scoring

The Court of Justice of the European Union addressed automated scoring in *OQ v. Land Hessen and SCHUFA Holding AG*, Case C-634/21.

The case concerned automated calculation of a probability value relating to an individual's ability to meet future payment obligations and the use of that score by third parties.²¹

The case illustrates the constitutional importance of automated scoring because the algorithmic output may become decisive in a subsequent decision affecting an individual's legal or economic position.

It therefore supports the broader proposition that algorithmic accountability cannot be limited to the entity that formally issues the final decision.

XIV. The German Constitutional Experience

The German Federal Constitutional Court's 1983 Census decision provides an important conceptual foundation even though it predates contemporary AI.

In that judgment, the Court developed the constitutional principle of informational self-determination, holding that individuals must in principle be able to determine the disclosure and use of their personal data.²²

The Court also emphasized that restrictions require a statutory basis consistent with the rule of law and proportionality, together with procedural safeguards against violations of personality rights.²³

The significance of the judgment for algorithmic transparency is indirect but substantial.

Modern algorithmic systems depend extensively upon personal data. Therefore, informational self-determination provides a constitutional bridge between traditional data protection and contemporary algorithmic governance.

XV. The American Experience

The American approach differs from the European model.

The United States lacks a single comprehensive federal AI regulation equivalent to the EU AI Act.

Nevertheless, constitutional and administrative principles can provide safeguards.

A. Due Process

Citron and Pasquale argue that automated scoring systems affecting important opportunities should be subjected to procedural safeguards, including meaningful opportunities for individuals to challenge erroneous classifications.²⁴

This approach is particularly relevant to algorithmic transparency because due process does not necessarily require access to source code. It may instead require sufficient information and procedures to enable meaningful challenge.

B. State v. Loomis

In *State v. Loomis*, 881 N.W.2d 749 (Wis. 2016), the Wisconsin Supreme Court considered the use of the COMPAS risk assessment system during sentencing.

The court allowed consideration of the risk assessment under specified conditions, while recognizing concerns associated with proprietary methodology and the limitations of algorithmic risk assessment.²⁵

The case demonstrates the difficulty of balancing proprietary interests against procedural fairness.

Its significance for the present study lies in the proposition that algorithmic decision-support systems may require procedural safeguards even where complete technical disclosure is unavailable.

XVI. The Jordanian Experience

A. Constitutional Foundations

Jordan does not currently recognize an express constitutional right entitled "the right to algorithmic transparency."

Nevertheless, several constitutional principles can support its development.

These include:

- equality;
- protection of individual rights and freedoms;
- privacy;
- freedom of expression;
- access to information;
- judicial protection;
- the rule of law.

The constitutional interpretation of these principles can evolve in response to digital transformation.

The absence of an explicit constitutional provision should therefore not be understood as the absence of constitutional protection.

XVII. Access to Information in Jordan

Jordan's access-to-information framework provides an important foundation for algorithmic transparency.

The Ministry of Justice continues to provide an official mechanism for submitting requests to obtain information.²⁶

However, traditional access-to-information legislation was not designed specifically for algorithmic decision-making.

The challenge is therefore to extend its application conceptually to information concerning:

- the existence of automated systems;
- their legal basis;
- their purpose;
- categories of data used;
- principal decision criteria;
- mechanisms for challenging outcomes.

This would represent a transition from document transparency to decision-process transparency.

XVIII. Jordan's Personal Data Protection Law No. 24 of 2023

Jordan's Personal Data Protection Law No. 24 of 2023 constitutes a significant development in the country's digital legal framework.

The law was officially published in Jordan's Official Gazette as Law No. 24 of 2023.²⁷

Its significance for algorithmic transparency arises from the close relationship between AI systems and personal-data processing.

Algorithmic accountability cannot be effectively achieved without regulating the data upon which algorithms operate.

The Jordanian framework can therefore be understood as developing through three interconnected layers:

Data Protection → Digital Governance → Algorithmic Accountability.

Nevertheless, the Personal Data Protection Law should not be presented as complete AI law. It provides an important foundation, but it does not by itself establish a comprehensive regulatory regime for all algorithmic decision-making.

XIX. The Jordanian Legislative Gap

Several areas remain in need of development.

First, Jordan lacks a comprehensive AI statute establishing a general governance framework.

Second, there is a need for specific rules governing automated administrative decisions.

Third, there is a need for algorithmic impact assessments where systems may significantly affect fundamental rights.

Fourth, public authorities require clear rules concerning human oversight.

Fifth, individuals require effective procedures for challenging significant automated decisions.

Sixth, courts and regulators require technical expertise sufficient to evaluate algorithmic systems.

The appropriate response is not to replace existing legislation but to develop an integrated framework connecting constitutional principles, data protection, administrative law, cybersecurity, and AI governance.

XX. The Role of Constitutional Courts

Constitutional courts may play a decisive role in the emergence of algorithmic transparency as a constitutional right.

A. Dynamic Constitutional Interpretation

Constitutional texts generally contain principles expressed at a level of abstraction capable of applying to new circumstances.

The concepts of:

- equality;
- dignity;
- privacy;
- liberty;
- due process;
- rule of law;

can therefore apply to technological systems even where the constitution predates artificial intelligence.

B. Constitutional Review of Algorithmic Legislation

A constitutional court may ask whether legislation authorizing automated decision-making adequately protects fundamental rights.

Relevant questions include:

1. Is the use of the algorithm authorized by law?

2. Are affected persons informed?
3. Can discriminatory outcomes be identified?
4. Is human intervention available?
5. Can the decision be challenged?
6. Is judicial review effective?
7. Are restrictions on transparency proportionate?

C. Proportionality

Proportionality is particularly important because algorithmic transparency frequently conflicts with legitimate interests.

A court should determine:

First, whether the restriction is prescribed by law.

Second, whether it pursues a legitimate objective.

Third, whether it is suitable to achieve that objective.

Fourth, whether it is necessary.

Fifth, whether the public benefit outweighs the infringement of individual rights.

This approach avoids the false choice between total transparency and total secrecy.

XXI. Proposed Constitutional Model

This article proposes five minimum constitutional guarantees.

1. Right to Notice

Individuals should be informed when a significant decision affecting their legal interests is substantially based upon automated processing.

2. Right to Meaningful Explanation

Individuals should receive understandable information concerning the principal factors and reasons materially contributing to the decision.

3. Right to Human Intervention

Where an automated decision has a significant impact on fundamental rights, the individual should have access to meaningful human review.

4. Right to Challenge

The affected person should be able to contest the decision and provide information capable of demonstrating error or unfairness.

5. Right to Effective Judicial Review

Individuals should have access to an independent and, where appropriate, judicial mechanism capable of reviewing the legality and fairness of the automated decision.

The proposed constitutional formula is:

Every person shall have the right to receive meaningful information and an understandable explanation concerning significant automated decisions affecting his or her rights or legal interests and shall have the right to challenge such decisions and request appropriate human review, subject to limitations prescribed by law and justified by legitimate interests in accordance with the principle of proportionality.

This formulation deliberately does not establish an absolute right to source code.

XXII. Findings

The study reaches the following findings:

1. Algorithmic transparency constitutes an emerging constitutional right, rather than an already universally recognized autonomous constitutional right.
2. Its constitutional foundations derive principally from the rule of law, equality, privacy, data protection, procedural fairness, access to information, and effective judicial protection.
3. Algorithmic transparency should not be equated with source-code disclosure.
4. Meaningful transparency is more appropriate than complete technical transparency.
5. Absolute transparency is neither technically feasible nor constitutionally necessary.
6. Relative and proportionate transparency provides a more balanced model.
7. The greater the impact of an automated decision on fundamental rights, the stronger the transparency and review obligations should become.
8. Article 22 GDPR provides important safeguards concerning certain solely automated decisions, including human intervention and contestation in specified circumstances.²⁸
9. The EU AI Act strengthens the European regulatory framework by introducing risk-based obligations and specific transparency requirements for high-risk AI systems.²⁹
10. The SyRI judgment demonstrates that existing human-rights guarantees can impose limits on opaque governmental algorithmic systems.³⁰
11. The German Census decision provides an important conceptual foundation for understanding the constitutional relationship between personal data and technological power.³¹
12. The American experience demonstrates that due-process principles can provide safeguards even without a comprehensive federal AI statute.

13. Jordan has significant constitutional and legislative foundations for developing algorithmic transparency.
14. Personal Data Protection Law No. 24 of 2023 represents an important component of this framework.³²
15. Jordan nevertheless requires a more comprehensive framework for AI and automated decision-making.
16. The most effective constitutional model should combine notice, explanation, human intervention, challenge, and judicial review.

XXIII. Recommendations

A. Constitutional Recommendations

1. Constitutional interpretation should recognize that existing fundamental rights apply to algorithmic decision-making.
2. Future constitutional reforms should consider expressly recognizing a right to meaningful information and explanation concerning significant automated decisions.
3. Any restriction on algorithmic transparency should satisfy legality and proportionality.

B. Legislative Recommendations

4. Jordan should consider adopting comprehensive legislation governing artificial intelligence and algorithmic decision-making.
5. AI systems should be classified according to risk.
6. High-risk systems affecting fundamental rights should be subject to enhanced transparency obligations.
7. Public authorities should conduct algorithmic impact assessments before deploying high-risk systems.
8. Legislation should expressly regulate the use of automated administrative decisions.

C. Institutional Recommendations

9. Independent mechanisms for algorithmic auditing should be established.
10. Data-protection authorities, cybersecurity institutions, administrative bodies, and courts should cooperate in supervising high-risk systems.
11. Public officials should receive specialized training in AI governance.

D. Judicial Recommendations

12. Individuals should have effective mechanisms for challenging significant automated decisions.

13. Courts should have authority to require disclosure of relevant algorithmic information where necessary for effective judicial review.

14. Judicial review should examine not only the final outcome but also the legality, fairness, and procedural integrity of the algorithmic process.

E. Technological Recommendations

15. Explainable AI should be incorporated into high-impact governmental systems.

16. Automated systems should maintain adequate audit trails.

17. Systems should be periodically tested for discrimination, accuracy, security, and compliance with fundamental rights.

F. Public Awareness

18. Citizens should be informed of their digital rights and the procedures available to challenge significant automated decisions.

19. Legal education should incorporate AI, algorithmic accountability, and digital constitutionalism.

XXIV. Conclusion

Artificial intelligence has introduced a new dimension to the exercise of public and private power. Automated decision-making can improve efficiency and administrative capacity, but it may simultaneously weaken traditional mechanisms of accountability when individuals cannot understand or challenge the processes that determine outcomes affecting them.

This study has argued that algorithmic transparency should be understood as an emerging constitutional right.

The proposed understanding does not require every constitution to immediately adopt an autonomous textual right to algorithmic transparency. Rather, the right can develop through the constitutional interpretation of existing principles, particularly the rule of law, equality, privacy, due process, access to information, and effective judicial protection.

The European experience demonstrates the practical importance of this development. The GDPR provides safeguards concerning certain forms of solely automated decision-making, while the AI Act establishes a broader risk-based framework and expressly requires appropriate transparency for high-risk systems.³³

Judicial developments reinforce this trend. The SyRI judgment demonstrates that an algorithmic governmental system may be subjected to fundamental-rights review because of inadequate transparency and verifiability.³⁴ The German Census decision, although predating AI, demonstrates how constitutional principles concerning informational self-determination can respond to technological transformations.³⁵

The American experience, particularly due process approaches to automated scoring, demonstrates another route: existing constitutional principles may impose procedural safeguards without requiring a comprehensive AI constitution.

Jordan presents a developing but promising case. The Constitution, access-to-information framework, and Personal Data Protection Law No. 24 of 2023 provide important foundations. However, these instruments should be supplemented by legislation specifically addressing AI governance and automated decision-making.

The central contribution of this article is therefore the proposal of Relative Algorithmic Transparency. The right should not be understood as a right to unlimited disclosure. Instead, the intensity of transparency should correspond to the seriousness of the automated decision and the degree to which fundamental rights are affected.

The constitutional minimum should consist of:

Notice + Meaningful Explanation + Human Intervention + Right to Challenge + Effective Judicial Review.

This model allows constitutional law to respond to technological transformation without sacrificing legitimate interests in privacy, intellectual property, cybersecurity, national security, and innovation.

Ultimately, the constitutional question is not whether algorithms should replace human decision-makers. It is whether the exercise of technologically mediated power can remain subject to constitutional accountability.

The answer proposed by this study is affirmative: no exercise of public power should become constitutionally unaccountable merely because it has been delegated to an algorithm.

Footnotes

1. See Joshua A. Kroll et al., *Accountable Algorithms*, 165 U. Pa. L. Rev. 633, 633–35 (2017). The authors explain that traditional legal accountability mechanisms may be inadequate when decisions formerly made by humans are delegated to computer systems.

2. See Regulation (EU) 2016/679, arts. 13–15, 22, 2016 O.J. (L 119) 1, 13–14, 43–44 (EU); Regulation (EU) 2024/1689, art. 13, 2024 O.J. (L), July 12, 2024.

3. See Danielle Keats Citron & Frank Pasquale, *The Scored Society: Due Process for Automated Predictions*, 89 Wash. L. Rev. 1, 1–4 (2014).

4. See Lilian Edwards & Michael Veale, *Slave to the Algorithm? Why a “Right to an Explanation” Is Probably Not the Remedy You Are Looking For*, 16 Duke L. & Tech. Rev. 18, 18–22 (2017).

5. Regulation (EU) 2016/679, art. 22, 2016 O.J. (L 119) 1, 43–44 (EU).

6. Regulation (EU) 2024/1689, art. 13, 2024 O.J. (L), July 12, 2024.

7. Personal Data Protection Law No. 24 of 2023, Official Gazette of the Hashemite Kingdom of Jordan (2023). The official Jordanian Gazette lists Law No. 24 of 2023 as the Personal Data Protection Law.
8. Citron & Pasquale, *supra* note 3, at 1–4.
9. Jenna Burrell, How the Machine “Thinks”: Understanding Opacity in Machine Learning Algorithms, 3 *Big Data & Soc’y*, no. 1, at 1–3 (2016).
10. Frank Pasquale, *The Black Box Society: The Secret Algorithms That Control Money and Information* 1–12 (Harvard Univ. Press 2015). The bibliographic details are confirmed by Harvard University Press's publisher record.
11. Kroll et al., *supra* note 1, at 633–35.
12. Edwards & Veale, *supra* note 4, at 18–22.
13. Brent Daniel Mittelstadt et al., The Ethics of Algorithms: Mapping the Debate, 3 *Big Data & Soc’y*, no. 2, at 1–10 (2016).
14. Sandra Wachter, Brent Mittelstadt & Chris Russell, Counterfactual Explanations Without Opening the Black Box: Automated Decisions and the GDPR, 31 *Harv. J.L. & Tech.* 841, 841–45 (2018). The authors argue that useful explanations can, in principle, be provided without disclosing the internal logic of the entire system.
15. Regulation (EU) 2024/1689, art. 13(1), 2024 O.J. (L), July 12, 2024.
16. Regulation (EU) 2016/679, art. 22(1)– (3), 2016 O.J. (L 119) 1, 43–44 (EU).
17. Sandra Wachter, Brent Mittelstadt & Luciano Floridi, why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation, 7 *Int’l Data Privacy L.* 76, 76–99 (2017).
18. Regulation (EU) 2024/1689, 2024 O.J. (L), July 12, 2024.
19. *Id.* art. 13.
20. *NJCM v. State of the Netherlands*, ECLI:NL: RBDHA:2020:865 (District Ct. The Hague Feb. 5, 2020). The court held that the SyRI legislation did not satisfy Article 8(2) of the European Convention on Human Rights and specifically found the system insufficiently transparent and verifiable.
21. *OQ v. Land Hessen & SCHUFA Holding AG*, Case C-634/21, ECLI:EU:C:2023:957 (C.J.E.U. Dec. 7, 2023).
22. Bundesverfassungsgericht [BVerfG] [Federal Constitutional Court], Dec. 15, 1983, 1 BvR 209/83 et al. (Census Act Case), ¶¶ 146–150 (Ger.). The Court recognized constitutional protection against unlimited collection, storage, use, and sharing of personal data and articulated informational self-determination.
23. *Id.*

24. Citron & Pasquale, *supra* note 3, at 1–4.
25. *State v. Loomis*, 881 N.W.2d 749, 753–57 (Wis. 2016). The case concerned the use of the COMPAS risk assessment tool in sentencing.
26. Ministry of Justice, Hashemite Kingdom of Jordan, *Right to Obtain Information*, official information-request form (2026).
27. Personal Data Protection Law No. 24 of 2023, Official Gazette of the Hashemite Kingdom of Jordan (2023).
28. Regulation (EU) 2016/679, art. 22.
29. Regulation (EU) 2024/1689, art. 13.
30. *NJCM v. State of the Netherlands*, ECLI:NL: RBDHA:2020:865.
31. BVerfG, 1 BvR 209/83 et al. (Dec. 15, 1983).
32. Personal Data Protection Law No. 24 of 2023, Official Gazette of the Hashemite Kingdom of Jordan.
33. Regulation (EU) 2016/679, art. 22; Regulation (EU) 2024/1689, art. 13.
34. *NJCM v. State of the Netherlands*, ECLI:NL: RBDHA:2020:865.
35. BVerfG, 1 BvR 209/83 et al. (Dec. 15, 1983).

Bibliography

A. Books

Frank Pasquale, *The Black Box Society: The Secret Algorithms That Control Money and Information* (Harvard Univ. Press 2015).

B. Journal Articles

Jenna Burrell, How the Machine “Thinks”: Understanding Opacity in Machine Learning Algorithms, 3 *Big Data & Soc’y*, no. 1, at 1–12 (2016).

Danielle Keats Citron & Frank Pasquale, The Scored Society: Due Process for Automated Predictions, 89 *Wash. L. Rev.* 1 (2014).

Lilian Edwards & Michael Veale, Slave to the Algorithm? Why a “Right to an Explanation” Is Probably Not the Remedy You Are Looking For, 16 *Duke L. & Tech. Rev.* 18 (2017).

Joshua A. Kroll et al., Accountable Algorithms, 165 *U. Pa. L. Rev.* 633 (2017).

Brent Daniel Mittelstadt et al., The Ethics of Algorithms: Mapping the Debate, 3 *Big Data & Soc’y*, no. 2 (2016).

Sandra Wachter, Brent Mittelstadt & Luciano Floridi, why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation, 7 *Int'l Data Privacy L.* 76 (2017).

Sandra Wachter, Brent Mittelstadt & Chris Russell, Counterfactual Explanations Without Opening the Black Box: Automated Decisions and the GDPR, 31 *Harv. J.L. & Tech.* 841 (2018).

C. European Union Legal Sources

Regulation (EU) 2016/679 of the European Parliament and of the Council of Apr. 27, 2016, *General Data Protection Regulation*, 2016 O.J. (L 119) 1.

Regulation (EU) 2024/1689 of the European Parliament and of the Council of June 13, 2024, *Artificial Intelligence Act*, 2024 O.J. (L), July 12, 2024.

D. Judicial Authorities

OQ v. Land Hessen & SCHUFA Holding AG, Case C-634/21, ECLI:EU:C:2023:957 (C.J.E.U. Dec. 7, 2023).

State v. Loomis, 881 N.W.2d 749 (Wis. 2016).

NJCM v. State of the Netherlands, ECLI:NL: RBDHA:2020:865 (District Ct. The Hague Feb. 5, 2020).

Bundesverfassungsgericht [BVerfG] [Federal Constitutional Court], Dec. 15, 1983, 1 BvR 209/83 et al. (Census Act Case) (Ger.).

E. Jordanian Legal Sources

Hashemite Kingdom of Jordan, *Constitution of the Hashemite Kingdom of Jordan* (1952, as amended).

Hashemite Kingdom of Jordan, *Right to Access Information Law No. 47 of 2007*.

Hashemite Kingdom of Jordan, *Personal Data Protection Law No. 24 of 2023*, Official Gazette (2023).

Hashemite Kingdom of Jordan, *Cybersecurity Law No. 16 of 2019*.

Hashemite Kingdom of Jordan, *Cybercrime Law No. 17 of 2023*.

F. International and Institutional Sources

Council of Europe, *Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law* (opened for signature Sept. 5, 2024). The Council of Europe describes the Convention as the first international legally binding treaty specifically addressing AI, human rights, democracy, and the rule of law.

UNESCO, *Recommendation on the Ethics of Artificial Intelligence* (Nov. 2021). UNESCO identifies transparency, fairness, human oversight, and human rights as central principles of its global AI ethics framework.