

HUMAN DIGNITY AND THE LEGITIMACY OF PUBLIC AUTHORITY IN THE DIGITAL TRANSFORMATION OF THE STATE: A TWO-AXIS GOVERNANCE TEST FOR AUTOMATED ADMINISTRATION

Svitlana Bobrovnyk

Department of Theory and History of Law and State
Educational and Scientific Institute of Law
Taras Shevchenko National University of Kyiv
Kyiv, Ukraine
ORCID iD: 0000-0002-9225-8871

Anatolii Shevchenko

Department of Law, Public Management, and Administration
Zhytomyr Polytechnic State University
Zhytomyr, Ukraine
ORCID iD: 0000-0003-2663-9892
shevchenko2757@ukr.net

Olha Varych

Department of Theory and History of Law and State
Educational and Scientific Institute of Law
Taras Shevchenko National University of Kyiv
Kyiv, Ukraine
ORCID iD: 0000-0003-0289-4039

Abstract.

The digital transformation of the state increasingly places public authority behind digital interfaces, data infrastructures, automated administrative procedures and artificial-intelligence-assisted decision systems. This article develops a theoretical-legal framework for assessing whether such transformation remains compatible with human dignity and with the legitimacy of public authority. It treats dignity as the substantive limit that prevents the individual from being reduced to a data object or passive object of administration, and legitimacy as the public-law condition that requires authority to remain intelligible, contestable, accessible and accountable when exercised through digital systems. Using doctrinal and comparative normative analysis, the article reads these concepts alongside European legal benchmarks, including the Charter of Fundamental Rights of the European Union, the General Data Protection Regulation, the EU Artificial Intelligence Act and Council of Europe instruments on algorithmic systems and artificial intelligence. The principal contribution is a two-axis governance test that translates dignity and legitimacy into operational questions for the design and review of digital public procedures. The test examines preservation of the person's legal subjecthood and individual circumstances, intelligibility of reasons, effective human review and remedy, equal accessibility, and identifiable institutional responsibility. The article argues that digitalisation strengthens public authority only when efficiency gains are accompanied by procedural safeguards, data protection, non-exclusion and meaningful avenues of challenge. The framework is conceptual rather than empirical and is offered as a normative assessment tool for sustainable digital governance.

Keywords: human dignity; legitimacy of public authority; digital transformation of the state; automated administration; AI governance; sustainable digital governance.

1. INTRODUCTION

The digital transformation of the modern state has become one of the principal ways in which the forms and methods of exercising public authority are changing in the twenty-first century. Its manifestations are the digitalisation of administrative procedures, the development of electronic services and of digital identification, the automated processing of data, the algorithmisation of administrative decisions, and the growing role of digital platforms in mediating the relationship between the state and the individual. The introduction of elements of artificial intelligence into public administration has substantially altered the character of that relationship.

Such processes are usually assessed through the prism of efficiency, speed, accessibility and institutional modernisation. Their effects, however, extend well beyond the technical renewal of public administration, and they cannot be evaluated solely as a technical modernisation of the state apparatus. Digitalisation bears directly on the value foundations of the modern state, because it changes the limits of authoritative influence, the degree of transparency of administrative decisions, the individual's access to the protection of their rights and interests, and the conditions under which public authority is recognised by society. In short, digital transformation alters not only the instruments of state activity but the character of public authority itself, the conditions under which it is perceived, and the limits of permissible authoritative interference.

The question that follows is whether the human being remains the centre of state policy under conditions of digitalisation, or whether the significance of the individual is gradually diminished and the person reduced to a digital profile or a set of data subject to automated processing. In this context, two categories acquire particular importance: human dignity and the legitimacy of public authority.

Human dignity makes it possible to assess whether digital transformation turns the person into a passive object of digital administration, and whether it reduces the person to a collection of data to be processed automatically. It is in this sense that dignity operates as a fundamental value of the modern state. Legitimacy, in turn, makes it possible to establish whether public authority retains social recognition under conditions in which authoritative procedures are becoming ever more complex, technologically mediated and potentially less intelligible to those subject to them. Digitalisation also changes the grounds of legitimacy. Whereas in the traditional understanding legitimacy was associated principally with legality, social recognition and trust in state institutions, digital transformation adds new criteria: the transparency of digital procedures, the accessibility of the substance of decisions taken by state bodies, the fairness of those decisions, and the possibility of oversight and appeal.

The central problem is therefore not whether the state should digitalise, but under what legal and institutional conditions digitalisation remains compatible with the status of the person as a rights-holder and with the justified exercise of public authority. A formally lawful digital procedure may still be normatively defective if it renders the person invisible as an individual, prevents them from understanding why a decision was taken, or leaves no effective human route for correction and challenge. Conversely, digitalisation may strengthen public authority where it expands access, reduces arbitrary discretion, improves traceability and preserves meaningful procedural guarantees.

This inquiry belongs squarely to the agenda of law, digital technologies and sustainable governance. Sustainable digital governance is understood here not as the persistence of a technical system but as the capacity of digitally mediated public authority to remain legally justified, socially recognisable, procedurally fair and institutionally accountable over time. Human dignity and legitimacy are therefore treated not as external ethical commentary on digital government but as internal conditions of its durability.

2. THE STATE OF RESEARCH AND THE RESEARCH GAP

Contemporary scholarship addresses e-government, automated administration, data protection, digital constitutionalism, algorithmic accountability and AI governance with considerable intensity. Yet three strands of the debate often remain separated. Human dignity is frequently invoked as a foundational value without being translated into concrete questions for system design; legitimacy is discussed as trust or social acceptance without sufficient connection to procedural safeguards; and technical or regulatory AI-risk frameworks do not always explain how defects in digital administration affect the justification of public authority as such. The resulting gap is therefore not a lack of discussion about digital government, but a lack of an integrated legal test linking the status of the person to the conditions under which digitally mediated authority can remain legitimate.

The present study addresses that gap through four propositions:

1. human dignity should operate as an assessable limit on the reduction of the person to data, categories or automated outputs;
2. legitimacy should be expressed through intelligibility, procedural fairness, accessibility, contestability and identifiable responsibility;
3. digital transformation should be evaluated against those two axes in addition to efficiency, legality and technical performance; and
4. a combined dignity–legitimacy test can be used *ex ante* when public bodies design digital procedures and *ex post* when their effects are reviewed.

3. AIM, SCOPE AND METHOD

The aim of the article is to substantiate human dignity and the legitimacy of public authority as interrelated criteria for assessing the digital transformation of the state and to operationalise those criteria in a two-axis governance test applicable to automated and algorithmically assisted public procedures. The study asks three questions: what dignity requires from digitally mediated authority; what conditions sustain legitimacy when decisions are technologically mediated; and how those requirements can be converted into practical design and review criteria.

Methodologically, the article proceeds by theoretical-legal (doctrinal) and comparative normative analysis. It reconstructs human dignity and legitimacy in general legal theory and tests those categories against contemporary forms of digital public authority. European legal materials are used as normative benchmarks: Article 1 of the Charter of Fundamental Rights of the European Union, the Charter's guarantees of good administration and effec-

tive remedy, the General Data Protection Regulation's rules on solely automated decisions with legal or similarly significant effects, the EU Artificial Intelligence Act, Council of Europe Recommendation CM/Rec(2020)1, and the Council of Europe Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law (CETS No. 225). As of August 2026, the EU AI Act has entered its general application phase, although specified obligations remain subject to staged dates. The study does not assume that each European instrument applies identically to every Ukrainian public body; they are used to identify converging principles relevant to comparative governance analysis. No original empirical data are presented, and the proposed test is normative rather than a validated psychometric or administrative-performance instrument.

4. HUMAN DIGNITY AS THE AXIOLOGICAL FOUNDATION OF THE MODERN STATE

4.1 DIGNITY AS A VALUE-BASED LIMIT ON PUBLIC AUTHORITY

Human dignity occupies a central place in the axiological structure of the modern state. It is not merely one legal value among many, but the normative and philosophical foundation on which the legitimacy of public authority must itself rest. In the contemporary understanding of statehood, dignity operates as the criterion that determines both the permissible limits of the exercise of public authority and the value orientation of legal regulation. For that reason, any analysis of the digital transformation of the state that ignores the role of human dignity risks remaining incomplete: it will reduce digitalisation to a purely technical or institutional process and pass over its profound effect on the legal status of the person (Charter of Fundamental Rights of the European Union, 2016; De Gregorio, 2022).

In legal theory, human dignity is traditionally understood as an inalienable quality of the person and as a principle shaping the relationship between the individual and the state. This understanding is reflected expressly in Article 1 of the Charter of Fundamental Rights of the European Union, which places dignity at the beginning of the Charter's normative architecture. For digital administration, the implication is not that every use of automation violates dignity, but that the person must remain a legal subject rather than becoming merely the object of classification, scoring or automated processing. The state may organise and modernise its institutions, but it must retain procedures capable of recognising rights, individual circumstances and legitimate interests (Charter of Fundamental Rights of the European Union, 2016; De Gregorio, 2022).

This understanding acquires particular significance where public authority relies on digital identity, linked databases, automated eligibility checks or AI-assisted administrative decisions. Data representations are necessarily selective: they describe the person through attributes that a system is designed to process. The legal risk arises when that representation becomes functionally equivalent to the person for decision-making purposes and no institutional mechanism remains for correcting incomplete data, presenting relevant circumstances or obtaining meaningful human reconsideration. European data-protection law addresses one part of this problem through safeguards surrounding certain decisions based solely on automated processing; these rules are not a general prohibition on automation, but they illustrate the broader requirement that significant decisions remain procedurally

governable (European Parliament and Council of the European Union, 2016; European Data Protection Board, 2018).

From an axiological standpoint, dignity therefore generates three requirements for digital public authority. First, the system must preserve legal subjecthood: the individual must be able to appear before the administration as more than a data profile. Second, the procedure must preserve agency: the person must be able to receive relevant information, submit material, correct data and seek human intervention where required by law. Third, technological mediation must remain proportionate to the public purpose pursued, particularly where biometric, behavioural, location or other intrusive data are involved. These requirements connect dignity to privacy, procedural fairness and the possibility of effective remedy without collapsing dignity into any one of those rights.

4.2 THE THREE FUNCTIONS OF HUMAN DIGNITY UNDER DIGITAL TRANSFORMATION

In this context it may be argued that human dignity performs at least three interrelated functions under conditions of the digital transformation of the state.

First, dignity operates as a foundational value of the modern legal order. It confirms that the legitimacy of state activity cannot be measured solely by efficiency, expediency or administrative rationality. Even where digital systems increase the speed and accessibility of administrative procedures, that alone cannot justify their use if they undermine the standing of the human being as an autonomous subject of law.

Second, dignity performs the function of a substantive limit on the digitalisation of public authority. Public authority cannot legitimately rely on digital systems in a manner that levels out the individual characteristics of the human being, the person and the citizen, or that makes it impossible to challenge individual decisions of state bodies effectively. In this sense dignity constrains the expansion of digital public authority, so that technological innovation remains compatible with the inalienable value of the human being.

Third, dignity serves as a criterion for assessing the admissibility of digital models of governance. It allows the question to be posed whether a particular digital system or platform is compatible with the value foundations of the modern state. Even where a digital procedure is formally permitted by law, it may nonetheless run counter to human dignity and may to some degree deprive the person of the realisation of their subjective rights and of the possibility of protecting them.

It follows that, where public authority relies on such systems, the human being becomes visible to the system only to the extent that they correspond to a predefined set of input data or to a predefined category — something that is capable, overall, of weakening the significance both of the human being and of legality in the relationship between the state and the individual. A state that organises digital public authority in such a way that people become invisible, interchangeable or procedurally defenceless risks undermining the very value foundation on which modern statehood rests.

The digital transformation of the state cannot, therefore, be regarded as axiologically neutral. It bears directly on the state's capacity to preserve its humanistic and legal orientation. Where digitalisation strengthens accessibility, transparency and procedural fairness

without eroding respect for the person, it can reinforce the value foundations of modern statehood. Human dignity should accordingly be regarded as the first and fundamental criterion for assessing the effectiveness of the digital transformation of public authority.

5. THE LEGITIMACY OF PUBLIC AUTHORITY IN THE DIGITAL AGE

Legitimacy concerns the justified recognition of public authority. In this article it is used in a normative public-law sense rather than as an empirical measure of popularity or trust. Digitalisation alters the conditions of legitimacy because the citizen increasingly encounters the state through interfaces, automated workflows and outputs generated from data rather than through an identifiable official exercising visible discretion. The question is therefore whether authority remains understandable, answerable and open to challenge when its exercise is technologically mediated.

Four conditions become especially important. The first is intelligibility: a person affected by a significant digital decision must be able to understand its legal and factual basis to the extent required for effective participation and challenge. The second is contestability: the procedure must preserve a realistic route to correction, review and remedy rather than merely provide a technically final output. The third is equal accessibility: digital-by-default administration must not convert lack of connectivity, disability, age, displacement or limited digital literacy into practical exclusion. The fourth is accountable attribution: responsibility must remain attached to an identifiable public institution and, where appropriate, to human decision-makers, rather than being displaced onto a vendor, dataset or model (Greenstein, 2022; Kouroutakis, 2024; Langer, 2024; Røhl, 2023).

A digitally transformed procedure may therefore comply with formal competence rules yet still suffer a legitimacy deficit if the person cannot understand the decisive grounds, cannot reach an effective reviewer, or cannot identify which authority is responsible for correcting an error. European law increasingly expresses these concerns through overlapping guarantees of good administration, data protection, transparency, human oversight and effective remedy. The EU AI Act and the Council of Europe Framework Convention on AI are significant not because they replace administrative law, but because they reinforce the proposition that technologically mediated authority must remain subject to human-rights, accountability and risk-management requirements (European Parliament and Council of the European Union, 2024; Council of Europe, 2024).

Legitimacy in the digital age should accordingly be understood as compatible with, rather than opposed to, efficiency. Faster services, reduced administrative burden and more consistent decisions may strengthen the justification of public authority when they are achieved within procedures that remain intelligible, inclusive and reviewable. The relevant distinction is therefore not between human and digital administration, but between governable and ungovernable digitalisation.

6. THE DUAL NATURE OF DIGITAL TRANSFORMATION

6.1 OPPORTUNITIES

Considered in its functional dimension, the digital transformation of the state opens up a number of evident opportunities.

The first is an increase in the promptness and effectiveness of public administration. Digital systems make it possible to reduce the time required to deliver services, to simplify administrative procedures, to reduce the bureaucratic burden, to increase the speed at which information is processed, and to optimise communication between public authorities and citizens. In this respect digitalisation contributes to the modernisation of the state mechanism and to the strengthening of its institutional capacity.

A second substantial opportunity is the widening of citizens' access to public services. Electronic services, digital personal accounts, remote forms of interaction with the state and electronic document flow are capable of making the realisation of rights and legitimate interests more convenient and faster, and less dependent on territorial or other organisational obstacles. In this respect digital transformation potentially strengthens the service orientation of the state and may be regarded as a way of bringing public authority closer to the needs of the individual (Røhl, 2023; da Rosa Lazarotto, 2025).

A further opportunity concerns the transparency of public authority. Where they are properly organised, digital instruments can facilitate access to public information, promote the openness of state registers, improve procedures for monitoring the activity of public bodies, and strengthen the capacity for public oversight — and thereby reduce corruption risks.

6.2 RISKS

Alongside these opportunities, however, the digital transformation of the state generates risks that are fundamentally new, and that are legal as well as axiological in character. Digitalisation cannot therefore be assessed exclusively as a positive instrument of modernisation. Its effect is dual in nature: on the one hand digital transformation opens new resources for the development of the modern state; on the other, it creates new threats to that state's humanistic, legal and democratic nature.

Depersonalisation of public authority. One of the most serious risks is the depersonalisation of public authority. The more the state's interaction with the individual is conducted through digital systems, the greater the probability that the person will be perceived by public authority not as an individualised subject of law but as a profile in a database or a set of formalised characteristics. Under such conditions public authority loses its immediate human dimension, and the legal relationship between the state and the individual is ever more extensively mediated by technological mechanisms. This creates the danger that the personal, individual and humanistic element will be progressively displaced from the sphere of public administration.

Identification of the person with their data. Closely connected with depersonalisation is the risk of identifying the person with their digital data. Where the individual comes to be

perceived primarily through a set of digital records, there is a danger that the real individual circumstances and the substance of the legal situation will fall outside proper consideration. Law then loses its just and human-centred nature.

Opacity of digital decisions. A person may receive a digital outcome without being able to identify the decisive factual inputs, legal rules or institutional reasoning behind it. The concern is not that every algorithm must be technically explainable to every user; the public-law requirement is that the administration remain capable of giving reasons sufficient for the affected person to understand and contest a decision where such reasons are legally required. Opacity becomes especially serious where automated or AI-assisted systems affect benefits, registration, licensing, taxation, migration, social support or other legally significant interests (Council of Europe, 2020; Greenstein, 2022; Langer, 2024).

Digital inequality. The risk of digital inequality requires particular attention. Not all persons possess the same level of digital literacy, technical access, stable connectivity, capacity to use electronic services or ability to understand digital procedures. Socially vulnerable groups, and persons located in the temporarily occupied territories of Ukraine, may find themselves in a situation in which formally accessible digital mechanisms in fact become a barrier. Digitalisation is thus capable not only of simplifying access to rights, but also of generating new forms of inequality in their realisation (Kouroutakis, 2024; da Rosa Lazarotto, 2025).

Expanded state supervision and control. Digital transformation expands the state's capacity to link datasets, infer behaviour and conduct large-scale monitoring. Such capacities may pursue legitimate public aims, but they also increase the risk of function creep, disproportionate surveillance and secondary uses of information unrelated to the purpose for which it was collected. A dignity-compatible digital state therefore requires purpose limitation, lawful data governance, proportionality and effective institutional oversight rather than an assumption that technical availability of data is equivalent to legal permission to use it.

Weakening of procedural protection. Simplification and automation can reduce administrative friction, but they must not eliminate notice, participation, correction of inaccurate data, reason-giving or access to review where those safeguards are required. Article 47 of the EU Charter provides an important European benchmark for effective remedy, while Article 22 GDPR illustrates the additional safeguards relevant to a defined category of solely automated decisions producing legal or similarly significant effects. The broader governance lesson is that digital convenience cannot be purchased by making the individual procedurally defenceless.

The digitalisation of the modern state is therefore a complex process that simultaneously opens new opportunities for improving the quality of public authority and generates new challenges to its legal and value-based nature.

7. A TWO-AXIS GOVERNANCE TEST FOR DIGITAL PUBLIC AUTHORITY

For the purposes of this study, the digital transformation of public authority is defined as the institutional, procedural and technological reorganisation of how state authority is

exercised through digital systems, assessed simultaneously against effectiveness, compatibility with human dignity and the capacity to preserve legitimate and accountable public decision-making. This definition moves the analysis beyond the adoption of technology and focuses on the legal quality of the authority exercised through it.

The principal practical contribution is a two-axis governance test. It is not intended to replace a data-protection impact assessment, AI risk assessment, judicial proportionality test or sector-specific legality review. Rather, it provides a common public-law structure for asking whether a digital procedure remains human-centred and institutionally justified before deployment and during subsequent audit.

Table 1. Two-axis governance test for digitally mediated public authority

Assessment dimension	Primary axis	Risk indicator	Governance safeguard
Legal subjecthood and individual circumstances	Dignity	Person reduced to a fixed data profile; no route to correct or supplement relevant information	Correction mechanisms; capacity to submit individual circumstances; human reconsideration where legally required
Privacy and proportionality of data use	Dignity	Function creep, excessive data linkage or intrusive monitoring unrelated to the administrative purpose	Purpose limitation; data minimisation; proportionality review; access controls and oversight
Intelligibility and reasons	Legitimacy	Affected person receives an outcome but cannot identify its legal or factual basis	Meaningful notice; reason-giving appropriate to the decision; documentation of decisive inputs and rules
Contestability and remedy	Both	No realistic route to challenge an automated or AI-assisted outcome	Accessible human review; correction and appeal mechanisms; preservation of effective remedy
Equal accessibility	Legitimacy	Digital channel excludes persons because of disability, displacement, connectivity or limited digital literacy	Accessible design; assisted and alternative channels; monitoring of exclusion effects
Accountability and traceability	Legitimacy	Responsibility is shifted to software, a model or an external vendor	Named responsible authority; audit logs; procurement controls; human oversight and incident accountability

Note. The test is an authorial conceptual synthesis based on the dignity and legitimacy framework developed in this article; it should be applied together with sector-specific legal requirements.

Applied ex ante, the dignity axis asks whether the proposed system preserves the status, agency and individual circumstances of the person. Public bodies should identify what data representation the system will use, whether affected persons can correct or supplement that representation, whether the system creates disproportionate monitoring or profiling risks, and where human intervention must remain available. This assessment is especially important where automated processing can materially affect rights, entitlements or access to public services.

The legitimacy axis asks whether the authority exercised through the system remains intelligible, contestable, accessible and attributable to a responsible institution. Efficiency is relevant but not decisive. A system that shortens processing time while making errors practically unchallengeable, excluding non-digital users or obscuring responsibility may improve administrative throughput while weakening legitimate governance.

Applied together, the two axes generate a governance rule: the more consequential the digital intervention for an individual's legal position, the stronger the requirements of reason-giving, human review, data governance, accessibility and auditability should become. This proportional relationship also provides a bridge between general legal theory and contemporary risk-based AI governance. Human dignity identifies what public authority must not lose sight of; legitimacy identifies the procedural and institutional conditions under which digitally mediated authority remains justified.

8. LIMITATIONS AND SCOPE OF APPLICATION

The proposed test is conceptual and normative. It does not measure public trust empirically, establish causal relationships between particular technologies and legitimacy, or determine the legality of a specific administrative system without reference to the law governing that system. Human dignity and legitimacy are contested concepts, and their concrete application will vary across legal orders and sectors.

The European instruments used in the analysis are comparative normative benchmarks rather than a claim of uniform direct applicability to Ukrainian public administration. Future research should therefore test the framework against concrete administrative domains, such as social benefits, taxation, licensing or digital identity, and should combine doctrinal analysis with user studies, administrative data and institutional audits. Such validation is necessary before the framework can be used as an empirical evaluation instrument.

9. CONCLUSIONS

The digital transformation of the modern state is not merely a technical renewal of administrative infrastructure. It changes how public authority sees the individual, how decisions are produced and explained, and how responsibility is allocated when public functions are mediated by data and automated systems. For that reason its success cannot be assessed by speed, convenience or cost reduction alone.

Human dignity operates as the substantive axis of assessment. It requires the digital state to preserve the person as a legal subject, to avoid treating a data profile as an exhaustive representation of the individual, and to retain procedures through which relevant circumstances can be presented, inaccurate information corrected and disproportionate data practices constrained. Dignity does not prohibit automation; it determines the conditions under which automation remains human-centred.

Legitimacy operates as the institutional and procedural axis. Digitally mediated authority remains justified where it is intelligible, contestable, accessible and attributable to a responsible public institution. A digital decision that cannot be effectively explained or challenged,

or a service that is formally available but practically inaccessible to significant groups, creates a legitimacy deficit even where the underlying technological system performs efficiently.

The two-axis governance test developed in this article translates those propositions into six operational dimensions: legal subjecthood and individual circumstances; proportional data use; intelligibility and reasons; contestability and remedy; equal accessibility; and accountability and traceability. Its scientific contribution lies in connecting the axiological category of dignity with the public-law category of legitimacy in a single assessment structure for digital administration.

The practical implication is a requirement of graduated safeguards. The more strongly a digital or AI-assisted procedure affects a person's legal position, the stronger the requirements for data governance, documentation, reason-giving, human review, accessibility and audit should be. This approach is compatible with the emerging European tendency toward risk-based AI regulation while retaining a specifically public-law focus on the justification of state authority.

Accordingly, sustainable digital governance should be understood as the capacity to preserve legitimate public authority through technological change. Digitalisation strengthens the state where it improves services while maintaining recognition of the person, effective legal protection and institutional responsibility. It undermines the state where technical efficiency is achieved through opacity, exclusion or procedural defenselessness. Future empirical and sector-specific research should test the proposed framework against real administrative systems and identify indicators capable of measuring how these safeguards operate in practice.

FUNDING

This research received no external funding.

CONFLICTS OF INTEREST

The authors declare no conflicts of interest.

ETHICS STATEMENT

This theoretical-legal study used publicly available legal and scholarly sources and did not involve human participants, personal data collection or experimental procedures; institutional ethics approval was therefore not required.

DATA AVAILABILITY

No original datasets were generated or analysed. All legal and scholarly materials used in the study are identified in the reference list.

REFERENCES

- Charter of Fundamental Rights of the European Union. (2016). Official Journal of the European Union, C 202, 389–405.
- Convention for the Protection of Human Rights and Fundamental Freedoms. (1950, November 4). Rome.
- Council of Europe. (2020). Recommendation CM/Rec(2020)1 of the Committee of Ministers to member States on the human rights impacts of algorithmic systems.
- Council of Europe. (2024). Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law (CETS No. 225). <https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treaty-num=225>
- da Rosa Lazarotto, B. (2025). The role of technology in citizens' right to good administration: Examining the impact of smart governments. In *Public governance and emerging technologies: Values, trust and regulatory compliance* (pp. 43–59). Springer. https://doi.org/10.1007/978-3-031-84748-6_3
- De Gregorio, G. (2022). Digital constitutionalism: An introduction. In E. Celeste & G. De Gregorio (Eds.), *Digital constitutionalism in Europe: Reframing rights and powers in the algorithmic society* (pp. 1–37). Cambridge University Press. <https://doi.org/10.1017/9781009071215.002>
- European Data Protection Board. (2018). Guidelines on automated individual decision-making and profiling for the purposes of Regulation 2016/679. https://www.edpb.europa.eu/documents/guideline/automated-decision-making-and-profiling_en
- European Parliament and Council of the European Union. (2016). Regulation (EU) 2016/679 of 27 April 2016 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). Official Journal of the European Union, L 119, 1–88. <https://eur-lex.europa.eu/eli/reg/2016/679/oj>
- European Parliament and Council of the European Union. (2024). Regulation (EU) 2024/1689 of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act). Official Journal of the European Union, L, 2024/1689. <https://eur-lex.europa.eu/eli/reg/2024/1689/oj>
- Greenstein, S. (2022). Preserving the rule of law in the era of artificial intelligence (AI). *Artificial Intelligence and Law*, 30(3), 291–323. <https://doi.org/10.1007/s10506-021-09294-4>
- Kouroutakis, A. E. (2024). Rule of law in the AI era: Addressing accountability and the digital divide. *Discover Artificial Intelligence*, 4, 115. <https://doi.org/10.1007/s44163-024-00191-8>
- Langer, C. (2024). Decision-making power and responsibility in an automated administration. *Discover Artificial Intelligence*, 4, 59. <https://doi.org/10.1007/s44163-024-00152-1>
- Røhl, U. B. U. (2023). Automated decision-making and good administration: Views from inside the government machinery. *Government Information Quarterly*, 40(4), 101864. <https://doi.org/10.1016/j.giq.2023.101864>