

THE RIGHT TO ADMINISTRATIVE OBLIVION AND BIOMETRIC DATA

PROTECTION IN THE PUBLIC SPACE: TOWARDS REBALANCING DIGITAL TRANSPARENCY AND CONSTITUTIONAL PRIVACY

Author: Dr. Mohamed Kamal Arafa Elrakhawi
Researcher, Consultant, Expert, Jurist, and Author
International Lecturer in Law and Intellectual Property Rights

Digital Object Identifier: 10.5281/zenodo.22082560

COPYRIGHT NOTICE

All rights reserved. Reproduction, translation, adaptation, or distribution in any form is strictly prohibited without the written permission of the author. All rights reserved for the first edition.

DEDICATION

To the souls of my pure father and pure mother, knowing that gratitude is not confined to blood and flesh, but extends to every ethical and legal act. May God grant them light in their graves and make them among the residents of Paradise.

To my beloved daughter with Spanish roots and Algerian heritage, who represents a future we build with just laws and a deeper human reality. May this effort placed in your hands be a methodology that illuminates your path with knowledge and justice.

RESEARCH ABSTRACT IN ENGLISH

Title: The Right to Administrative Oblivion and Biometric Data Protection in the Public Space: Towards Rebalancing Digital Transparency and Constitutional Privacy

Executive Summary: This work examines the fundamental transformation imposed by the right to administrative oblivion on the structure of public records and traditional data protection theories. It discusses the inadequacy of absolute archiving models in accommodating the permanent nature of biometric data, and proposes the theory of digital administrative limitation as a new legal framework balancing transparency and anti-corruption with human dignity and privacy. Employing a critical analytical and comparative methodology, integrating digital law philosophy and applied ethics, it presents a comprehensive legislative and judicial framework ensuring citizen protection, stimulating administrative innovation, and preserving the principles of the rule of law in the digital age.

Keywords: Administrative Oblivion, Biometric Data, Digital Limitation, Administrative Archiving, Constitutional Privacy, Digital Redaction Right, Transparency-Privacy Balance

Research Problem: How can public administration reconcile its legal duty to maintain digital archives for transparency and corruption prevention with the citizen constitutional right to erase

digital administrative footprints and forgetfulness after the purpose is fulfilled? What legal safeguards are necessary to protect biometric data from exploitation or unjustified permanent storage?

Methodology: Critical analytical methodology of legislative texts and administrative-constitutional rulings, advanced comparative methodology covering EU, France, South Korea, and Brazil experiences, and an interdisciplinary methodology integrating administrative law with data philosophy, digital ethics, and human rights.

Results: Inapplicability of traditional archiving laws to biometric data, necessity of adopting conditional digital administrative limitation theory, viability of digital redaction as an alternative to absolute erasure in public interest cases, and urgent need for independent regulatory bodies overseeing the lifecycle of vital data.

Conclusion: Transitioning to an administrative system recognizing digital forgetfulness is not a retreat from transparency, but a constitutional evolution preserving human dignity in the digital age, requiring clear legislation defining storage periods, erasure conditions, oversight mechanisms, and effective judicial guarantees preventing transition to permanent administrative surveillance.

INTRODUCTION

The emergence of the right to administrative oblivion and biometric data protection constitutes one of the deepest constitutional and legal transformations witnessed in the digital age. Administration has shifted from a model relying on limited, destructible paper records to a reality where massive databases, permanent biometric data, and continuous digital archives intertwine, fundamentally shaking the foundations of traditional theories of transparency, anti-corruption, and individual privacy. The core research problem is not limited to the technical efficiency of data collection, but extends to obscuring the relationship between the digital state and the citizen, the nature of administrative oversight, sources of accountability, and guarantees of rights in systems that may retain sensitive biological identifiers far beyond real-time human oversight.

The author proceeds from a central hypothesis: that the traditional model based on the duality of absolute archiving or complete deletion was not designed to absorb biometric permanence, thus necessitating a transition to a new legal framework based on the theory of conditional digital administrative limitation, the right to digital erasure, intelligent masking tools, and specialized judicial oversight. This work aims to present an integrated legislative and jurisprudential framework that balances protecting affected parties, promoting administrative innovation, and preserving the principles of the rule of law, without falling into excessive restriction or reckless abandonment of constitutional guarantees.

The scope of this framework primarily targets civil administrative records, such as social security, taxation, and licensing databases, while acknowledging that criminal justice archives

require distinct, stricter constitutional protocols. The methodological structure is designed as a sequential book of twenty chapters, moving from theoretical derivation through critical analysis of existing models to legislative proposals, data protection mechanisms, and digital legality oversight, with continuous linkage to comparative experiences and institutional requirements. The work concludes with a foundational conclusion that outlines pathways for future legal development, emphasizing that digital administrative law is not merely a technical branch but a profound transformation in the concepts of authority, accountability, and administrative justice. Acknowledging the nature of biometric data as an extension of human identity does not mean abandoning administrative transparency, but rather re-formulating oversight, guarantee, and limitation tools in a manner consistent with the reality of the digital age while maintaining the delicate balance between administrative efficiency and citizens rights.

Defining the Digital-Biometric Public Space:

In this research, the Public Space is conceptualized not merely as the physical realm of streets and squares subjected to biometric surveillance, nor solely as the administrative domain of public registries. Rather, it is defined as the Digital-Biometric Public Sphere, the intersection where physical biological identifiers are continuously extracted, processed, and archived by public administration. This dual nature necessitates a legal framework that governs both the spatial surveillance of the citizen and the temporal archiving of their biological identity.

This work aspires to be a methodological reference for researchers, legislators, judges, and administrative practitioners in building a resilient, just, and digitally-adaptable administrative system capable of continuous development.

CHAPTER ONE: The Theoretical Framework and Jurisprudential Derivation of the Right to Administrative Oblivion

The definition of the right to administrative oblivion constitutes the central axis from which any jurisprudential analysis of digital archiving proceeds. Traditional jurisprudence and judiciary have stabilized around known elements: the priority of preserving administrative records, accountability and transparency, and the citizen right to defense. However, the entry of biometric data and digital accumulation into administrative operations has produced fundamental disruptions in the element of temporal limitation.

By distinguishing traditional elements of administrative archiving from the unique demands of biometric data, this section establishes a new definition of digital administrative limitation. This definition is intrinsically linked to purpose completion, the absence of overriding public interest, and robust digital masking guarantees. Ultimately, recognizing conditional digital administrative limitation as a formal legal principle paves the way for a comprehensive restructuring of administrative data protection, provided it meets conditions of institutional recognition, regulatory transparency, and subjection to legality oversight.

CHAPTER TWO: Development of the Concept of Constitutional Privacy in the Digital Transformation of Administration

Constitutional privacy is historically considered a fundamental right covering residence, correspondence, and private life. In the digital age, it has expanded to include personal data, digital identity, and electronic records.

Through critical analysis of comparative models, this section demonstrates that constitutional privacy has not remained confined to material isolation, but has expanded to serve functional and digital guarantee purposes. This justifies proposing a model of dynamic functional privacy as a positive right encompassing control over data, the right to know, the right to correction, and the right to oblivion. The chapter links acknowledgment of limited digital privacy to building an integrated system of digital administrative oversight where functional privacy becomes a guarantee tool rather than an ontological end, facilitating determining oversight boundaries, accelerating accountability, and preserving human dignity.

CHAPTER THREE: Limitations of Absolute Archiving Theory in Facing Biometric Permanence

Absolute archiving theory in administration links historical preservation to direct administrative continuity, which facilitates establishing institutional memory and determining legal precedent. However, this model fundamentally stumbles before biometric data systems that retain permanent biological identifiers and develop their analytical patterns autonomously over time.

This theoretical limitation is vividly illustrated by real-world jurisprudence, such as the landmark 2020 SyRI case in the Netherlands, where the District Court of The Hague invalidated an administrative algorithmic risk-scoring system for violating the right to privacy under Article 8 of the European Convention on Human Rights. Similarly, the French Conseil d'Etat has repeatedly restricted the use of biometric data in public services, such as schools, emphasizing that administrative efficiency cannot override fundamental constitutional privacy. Analytically, proving institutional necessity for permanent retention becomes quasi-impossible in the face of biometric data with continuous analytical potential, necessitating a transition to a conditional or hybrid retention model.

CHAPTER FOUR: Traditional Data Protection Theory and Challenges of Machine Learning in Administration

Administrative judiciary has stabilized on traditional data protection theory as an objective safeguard based on defined retention periods and purpose limitation, without need to prove individual harm. However, this theory assumes stable administrative boundaries, continuous human oversight, and ability to accurately identify the lifecycle endpoint.

Addressing the core problem of continuous learning, this chapter demonstrates that harm in data processing is no longer confined to manual misuse or institutional procedure, but may arise from deviation of algorithms from their programmed objectives, unexpected interaction with new environmental variables, or distortion of training data. Methodologically, the chapter relies on comparing traditional protection standards with proposed digital standards, analyzing the role of

algorithmic audit and audit logs, and linking this to the rapid erasure mechanism, thereby building an independent electronic oversight capacity that guarantees compliance without delay.

CHAPTER FIVE: Hybrid Oversight Model Between Institutional Accountability and Digital Limitation

The hybrid oversight model is considered an intermediate solution that combines advantages of traditional administrative transparency with flexibility of digital privacy guarantees, balancing protection of affected parties and promoting administrative innovation, while limiting unexpected institutional surveillance costs.

Analytically, the hybrid model rests on three fundamental pillars: first, determining the administrative body responsible for retention, monitoring, and oversight; second, establishing limited electronic retention periods funded from licensing requirements, compliance certifications, and periodic review mandates; third, guaranteeing rapid compliance without proving direct personal harm. The chapter links the hybrid model to the necessity of developing specialized supervisory tools, concluding that it represents the optimal framework for managing digital administrative risks.

CHAPTER SIX: Digital Erasure Mechanisms: Legal Structure and Enforcement Procedures

The administrative digital erasure mechanism constitutes the executive guarantee tool for ensuring compliance with the right to oblivion, without recourse to lengthy judicial procedures, proving individual harm, or disrupting the course of public records.

Methodologically, the chapter designs a complete operational model for erasure including: request procedures, verification steps, technical execution, external audit, and linking erasure processes to clear objective standards.

The Imperative of Machine Unlearning:

Traditional data erasure mechanisms are insufficient in the era of administrative machine learning. If biometric data has been ingested to train an administrative algorithm, deleting the raw database does not erase the algorithmic memory of that data. Therefore, the digital redaction mechanism must legally mandate Machine Unlearning, a technical and legal obligation requiring the developer or administration to mathematically isolate and remove the influence of the specific biometric data from the trained model, ensuring that the right to oblivion extends from the database to the algorithmic weights themselves.

CHAPTER SEVEN: Algorithmic Audit Standards and Transparency of Administrative Data Policies

Transparency of algorithms and data retention policies is considered a fundamental condition for legal accountability, judicial oversight, and protection of administrative defense rights.

However, technical complexity and intellectual property rights and cybersecurity risks always create tension between full disclosure and complete transparency.

By analyzing organizational models for audit across multiple jurisdictions, this chapter proposes a legal framework for graduated audit linked to official recognition, prior oversight, and judicial appeal mechanisms. Algorithmic audit does not necessarily mean revealing source code in its entirety, but includes disclosure of retention criteria, system objectives, limitation limits, training data sources, verification mechanisms, and audit logs.

CHAPTER EIGHT: The Problem of the Algorithmic Black Box and Challenges of Legality Oversight

The complexity of algorithms and their inability to be fully interpreted by humans, especially in advanced biometric processing systems, represents one of the deepest challenges facing administrative legality oversight.

Addressing the administrative and judicial challenges of algorithmic opacity, this chapter proposes alternative oversight tools relying on pattern analysis, monitoring normative deviation, statistical distortion analysis, and obliging administration to provide simplified and reviewable explanations.

Zero-Knowledge Archiving as a Balancing Tool:

To resolve the paradox between the Right to Administrative Oblivion and the Principle of Administrative Transparency and Anti-Corruption, this framework proposes the adoption of Zero-Knowledge Archiving. This is technically operationalized through advanced cryptographic protocols such as Zero-Knowledge Succinct Non-Interactive Arguments of Knowledge (zk-SNARKs) or Homomorphic Encryption. These mechanisms allow the administration to verify the validity and integrity of an administrative act without ever decrypting or accessing the underlying biometric hash. Furthermore, to safeguard against future "Store Now, Decrypt Later" threats, this long-term archival must adopt Post-Quantum Cryptography (PQC) standards, ensuring that the cryptographic vault remains impervious to future quantum computing decryption capabilities. The sealed proof remains accessible exclusively via a multi-signature judicial key in cases of proven corruption or serious crimes, thereby harmonizing human dignity with the public right to accountability.

CHAPTER NINE: The Role of Administrative Judiciary in Developing Algorithmic Compliance Oversight

Administrative judiciary represents the final explicit guardian of the principle of legality, stability of the public fund, and rights of affected parties. However, its traditional nature based on reviewing formal and substantive legality faces tangible challenges before complex and non-fully-interpretable biometric processing decisions.

Recognizing that algorithmic compliance oversight does not require the judge to become a technical expert, this chapter focuses on developing normative review tools. This includes reviewing system objectives, design standards, retention limits, audit logs, and reliance certifications, focusing on reviewing outputs and their compliance with legal principles, proportionality, defense rights, and the balance principle.

CHAPTER TEN: Administrative and Judicial Appeal Mechanisms in the Presence of Digital Administrative Systems

Administrative and judicial appeal mechanisms constitute fundamental guarantees for protecting rights, correcting deviation, and maintaining balance between administrative efficiency and decision justice.

To address the profound procedural challenges in the digital environment, this chapter designs a complete methodology for digital appeal including: stages of administrative injustice, technical review, judicial appeal, precautionary suspension mechanisms, and rapid compliance standards. This links to the competencies of independent supervisory bodies and the role of administrative judiciary in subsequent oversight.

CHAPTER ELEVEN: The Role of Independent Supervisory Bodies in Overseeing Administrative Artificial Intelligence

Independent supervisory bodies represent a fundamental pillar in balancing technology, oversight, and rights protection in complex digital environments.

Analytically, this chapter demonstrates that an independent supervisory body requires broad competencies including: prior recognition, periodic audit, official accreditation, imposing transparency standards, imposing exemplary sanctions, precautionary suspension for high-risk systems, and cooperation with administrative judiciary in joint oversight, while guaranteeing financial, administrative, and technical independence.

CHAPTER TWELVE: Standards of Official Recognition and Prior Licensing for Intelligent Administrative Systems

Official recognition and prior licensing represent fundamental preventive tools for ensuring compliance of intelligent systems with legal, ethical, and technical standards before their integration into the administrative structure.

Furthermore, this accreditation framework directly aligns with the stringent requirements of the European Union Artificial Intelligence Act (EU AI Act, 2024). Specifically, it operationalizes Article 9 (Risk Management Systems) and Article 15 (Accuracy, Robustness, and Cybersecurity), while mandating the Fundamental Rights Impact Assessment (FRIA) that is strictly required for the deployment of high-risk AI systems within public administration.

CHAPTER THIRTEEN: Liability of Developer and Operator in the Digital Administrative Environment

Liability of developer and operator represents a profound element in the chain of digital accountability. However, complexity of systems, multiplicity of participating parties, and nature of self-learning produce obscurity in determining the liable party in case of administrative or algorithmic error.

By analyzing comparative liability models, this section proposes clear standards for distributing liability including: developer liability for design and data, operator liability for operation and monitoring, and administration liability for accreditation and oversight, linking this to shared compensation mechanisms, graduated sanctions, and financial guarantees.

CHAPTER FOURTEEN: Digital Administrative Contracts and Conditions of Normative Compliance

Administrative contracts represent the fundamental contractual tool for regulating relationship between administration and developer or operator.

Analytically, the chapter demonstrates that a digital administrative contract requires clear standards including: legal definitions, transparency standards, independence limits, liability for cybersecurity, update mechanisms, data transparency, accreditation standards, conditions for revoking accreditation, shared compensation mechanisms, and periodic review clauses.

Mandatory Algorithmic Impact Assessment:

No digital administrative contract shall be deemed valid or normative unless accompanied by a prior, independent Algorithmic Impact Assessment. This assessment must evaluate the system potential impact on constitutional privacy, the risk of biometric distortion, and the proportionality of data retention, serving as a mandatory annex that conditions the official recognition and licensing of the intelligent system.

CHAPTER FIFTEEN: The Role of Applied Ethics in Regulating Administrative Artificial Intelligence

Applied ethics represent a fundamental guiding framework for ensuring compliance of intelligent systems with human values, human rights, and principles of administrative justice.

By analyzing internationally recognized ethical principles, this chapter proposes a model for integrating ethics with legislation through executive charters, linking ethics to contracts, accreditation standards, oversight criteria, and judicial accountability mechanisms. The chapter concludes that applied ethics need to be transformed from a guiding framework to a binding legal standard.

CHAPTER SIXTEEN: Impact of Artificial Intelligence on the Principle of Equality Before the Public Fund

The principle of equality before the public fund represents a fundamental axis in administrative law, guaranteeing equal treatment of citizens under same conditions. However, artificial intelligence systems may produce unintended discrimination resulting from data distortion, unbalanced design standards, or unexpected interaction with demographic or social variables.

Moreover, substantive equality in the digital age transcends formal identical treatment. It necessitates proactive "Training Data Audits" and continuous monitoring for "Statistical Fairness." This ensures that algorithmic models do not inadvertently reproduce or amplify historical, structural discrimination against marginalized demographic groups, thereby transforming the principle of equality into a dynamic, verifiable administrative obligation.

CHAPTER SEVENTEEN: The Role of Artificial Intelligence in Developing Digital Public Service

Digital public service represents a fundamental practical field for integrating artificial intelligence in administration, where efficiency improvement, procedure acceleration, error reduction, and increased citizen satisfaction are expected.

Addressing the practical problem of unregulated application, this chapter demonstrates that digital public service needs clear design standards including: ease of use, transparency of standards, independence limits, cybersecurity standards, and human support mechanisms. The chapter relies on designing a complete model for digital service including development stages, testing, accreditation, operation, review, and update.

CHAPTER EIGHTEEN: Impact of Artificial Intelligence on Administrative Transparency and Combating Corruption

Administrative transparency represents a fundamental tool for guaranteeing accountability, building citizen confidence, and combating corruption. However, complexity of algorithms, absence of source disclosure, and inability for full interpretation may produce organizational obscurity.

By designing a complete digital transparency framework, this chapter demonstrates that transparency in the digital age includes algorithmic oversight, monitoring standards, audit logs, and decision review, linking this to accountability principles, defense rights, and effective judicial oversight.

CHAPTER NINETEEN: Horizons of Digital Administrative Legislation in the Coming Age

Digital administrative legislation represents the fundamental legal framework for regulating use of artificial intelligence in administration, guaranteeing legality, protecting rights, and managing risks.

Analytically, this chapter demonstrates that digital administrative legislation requires clear standards including: legal definitions, accreditation standards, independence limits, audit mechanisms, liability of developer and operator, independent supervisory bodies, rapid compensation mechanisms, and digital legality oversight. The chapter relies on designing a complete legislative structure including framework law, executive charters, technical standards, and mechanisms linked to administrative judiciary.

CHAPTER TWENTY: Final Recommendations and Foundational Conclusion

The author concludes this work with a methodological emphasis on the necessity of transitioning from traditional administrative models to the standing digital environment. Autonomous artificial intelligence is not merely a technical transformation but a fundamental redefinition of administrative decision concept, legality, liability, and judicial oversight.

This work aspires to be a hesitant but methodological step toward a more just, more transparent, and more capable digital administrative system of absorbing complexity of the digital age in all its dimensions. Questions and debate remain alive, and living administrative law is what forms with each new generation of technologies.

The transition to digital administrative oblivion is not a technical downgrade, but a constitutional upgrade that transforms the citizen from a mere data subject into a sovereign biological entity in the eyes of the digital state.

RESEARCH ABSTRACT IN FRENCH

Titre: Le droit à l'oubli administratif et la protection des données biométriques dans l'espace public: vers un rééquilibrage entre transparence numérique et vie privée constitutionnelle

Resume executif: Ce travail examine la transformation fondamentale imposée par le droit à l'oubli administratif sur la structure des archives publiques et les théories traditionnelles de protection des données. Il distingue clairement entre le concept judiciaire plus large du "Droit à l'oubli" et le mécanisme réglementaire spécifique du "Droit à l'effacement" (conformément à l'article 17 du RGPD). Il discute de l'inadéquation des modèles d'archivage absolu pour accueillir la nature permanente des données biométriques, et propose la théorie de la limitation numérique administrative comme nouveau cadre juridique équilibrant transparence et lutte contre la corruption avec la dignité humaine et la vie privée.

Mots-cles: Oubli administratif, droit à l'effacement, données biométriques, limitation numérique, archivage administratif, vie privée constitutionnelle, équilibre transparence-vie privée

Problématique de recherche: Comment l'administration publique peut-elle concilier son devoir légal de conserver les archives numériques pour la transparence et la lutte contre la corruption avec le droit constitutionnel du citoyen d'effacer ses traces administratives numériques et

d'oublier apres realisation de l'objectif? Quelles garanties juridiques sont necessaires pour proteger les donnees biometriques de l'exploitation ou du stockage permanent injustifie?

Methodologie: Methode analytique critique des textes legislatifs et jurisprudence administrative-constitutionnelle, methode comparee avantee couvrant les experiences UE, France, Coree du Sud et Bresil, et methode interdisciplinaire integrant le droit administratif avec la philosophie des donnees, l'ethique numerique et les droits humains.

Resultats: Inapplicabilite des lois d'archivage traditionnelles aux donnees biometriques, necessite d'adopter la theorie de la limitation numerique administrative conditionnelle, viabilite du masquage numerique comme alternative a l'effacement absolu dans les cas d'interet public, et besoin urgent d'organismes de regulation independants surveillant le cycle de vie des donnees vitales.

Conclusion: Le passage vers un systeme administratif reconnaissant l'oubli numerique n'est pas un retrait de la transparence, mais une evolution constitutionnelle preservant la dignite humaine a l'ere numerique, exigeant une legislation claire definissant les delais de stockage, les conditions d'effacement, les mecanismes de controle, et des garanties judiciaires efficaces empechant la transition vers une surveillance administrative permanente.

Author: Dr. Mohamed Kamal Arafa Elrakhawi
Researcher, Consultant, Expert, Jurist, and Author
International Lecturer in Law

Copyright Reserved for the Author
Reproduction, adaptation, translation, or distribution in any form is strictly prohibited without written permission from the author.

First Edition: 2026
Digital Object Identifier: 10.5281/zenodo.22082560

APPENDICES

APPENDIX A: GLOSSARY

Administrative Oblivion: The right of a citizen to have their digital administrative footprint functionally limited or erased after the fulfillment of the administrative purpose.

Machine Unlearning: A technical and legal obligation requiring the mathematical isolation and removal of the influence of specific data from a trained machine learning model.

Zero-Knowledge Archiving: A cryptographic method allowing verification of data integrity without accessing the underlying raw data, often utilizing zk-SNARKs or Homomorphic Encryption.

Post-Quantum Cryptography (PQC): Cryptographic algorithms designed to be secure against an attack by a quantum computer, essential for long-term biometric data archival.

APPENDIX B: MODEL LEGISLATIVE CLAUSES AND LIABILITY MATRIX

Model Legislative Clause on Machine Unlearning:

Article X: Right to Algorithmic Erasure. Any natural person has the right to request the complete erasure of their biometric data from active administrative databases and the execution of Machine Unlearning protocols to remove the influence of such data from trained administrative algorithms, within thirty days of the fulfillment of the administrative purpose, unless a final judicial ruling dictates otherwise.

Model Legislative Clause on Post-Quantum Archiving:

Article Y: Long-Term Biometric Security. All archived biometric data subject to conditional retention must be secured using Post-Quantum Cryptography (PQC) standards to guarantee perpetual protection against future cryptographic vulnerabilities and "Store Now, Decrypt Later" attacks.

Liability Distribution Framework:

1. Design Flaw or Inherent Algorithmic Bias: Primary liability rests with the Developer, who must guarantee the structural integrity and fairness of the model.
2. Data Poisoning or Improper Input: Primary liability rests with the Operator or Public Administration, responsible for the quality and legality of the data fed into the system.
3. Failure to Audit or Monitor: Joint liability rests with the Independent Supervisory Body and the Public Administration for neglecting ongoing compliance verification.
4. Unauthorized Access or Breach: Liability rests with the entity failing to maintain mandated cybersecurity and Zero-Knowledge Archiving standards.

REFERENCES

1. Bourtoutle, L., et al. (2021). Machine Unlearning. IEEE Symposium on Security and Privacy.
2. European Union. (2024). Artificial Intelligence Act (Regulation (EU) 2024/1689).
3. Conseil d'Etat. (2021). Decision regarding the use of biometric data in educational institutions.
4. District Court of The Hague. (2020). SyRI case (System Risk Indication), ECLI:NL:RBDHA:2020:865.
5. European Data Protection Board (EDPB). (2023). Guidelines on the processing of biometric data for the purpose of identification in the context of the GDPR.
6. Mayer-Schönberger, V. (2011). Delete: The Virtue of Forgetting in the Digital Age. Princeton University Press.
7. Cate, F. H., & Mayer-Schönberger, V. (2013). Notice and Consent in a World of Big Data. International Data Privacy Law, 3(1), 3-11.
8. Zarsky, T. (2016). The Trouble with Algorithmic Decisions: An Analytic Road Map to Examine Efficiency and Fairness in Automated and Opaque Decision Making. Science, Technology, & Human Values, 41(1), 118-132.
9. Solove, D. J. (2013). Privacy Self-Management and the Consent Dilemma. Harvard Law Review, 126(7), 1880-1903.

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