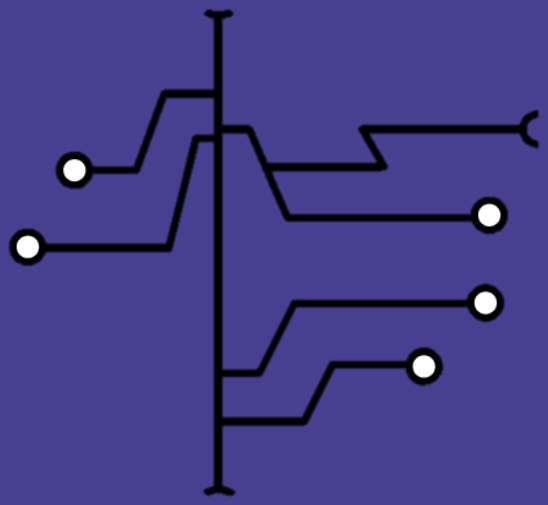

SOCIAL PROTECTION, DISCRIMINATION AND AUTOMATION

Bojana Kostić, Ana Toskić Cvetinović

Social Protection, Discrimination and Automation:

Everything that could go wrong, went wrong.

For the Publisher:
Nađa Marković

Authors:
Bojana Kostić
Ana Toskić Cvetinović

Translation:
Tamara Vlahović Šanović

Design and prepress:
Gorica Nikolin

Belgrade, October 2025

www.a11initiative.org
office@a11initiative.org

This report was produced as part of a project supported by the Digital Freedom Fund. The views, analyses, and conclusions expressed herein are those of the authors and do not necessarily reflect the views of the Digital Freedom Fund. Responsibility for the content of this publication lies entirely with the authors.

Table of Content

1. Introduction

The research titled *"Social Protection, Discrimination and Automation: Everything that Could Go Wrong, Went Wrong"* applies a comparative legal analysis to examine both general and specific regulations in various predominantly European nations (with the exception of Canada) shedding light on existing legal measures that, although still in their early stages, seek to mitigate the harmful effects of automated decision-making systems. Based on past experiences and the very nature of these systems, the literature suggests that their indirect purpose amounts to the "criminalization of poverty,"[1] as decisions are predominantly made about, and impact the lives of, vulnerable groups. The need for this research is becoming increasingly evident every day. The current focus of the study is the Social Card system[2], though the findings are also relevant to other forms of automation of public administration that have been gaining ground in Serbia in recent years, particularly regarding the cross-referencing of data from different databases and public registers,[3] as well as the use of artificial intelligence systems.[4]

From this perspective, the research **aims** to analyze comparative legal frameworks governing administrative decision-making through algorithmic systems. Particular emphasis is placed on safeguards for vulnerable groups, insofar as the legislative frameworks of the analyzed countries specifically address these concerns. The study does not focus exclusively on the regulation of algorithmic social protection systems in European countries but also examines other automated systems, including artificial intelligence (AI), in the context of access to and the fulfillment of economic and social rights, such as the rights to housing, healthcare, employment, etc.

Relying on diverse **methodological approaches**, this research emphasizes particular legal thematic areas of protection that have demonstrated significance in

---

[1] See also O'Neil - Weapons of Mass Destruction and V. Eubank Automating Inequality. See, for example: J. Niklas, Human Rights Based Approach to AI and Algorithms, in The Law of Algorithms, edited by W. Barfeild, Cambridge University Press, 2020, p.24-

[2] Social Cards, Ministry of Labor, Employment, Veteran and Social Affairs. Available at: https://www.minrzs.gov.rs/sr/projekti/prioriteti/socijalne-karte

[3] As early as 2019, the introduction of artificial intelligence by the Tax Administration was announced, intended for analyzing taxpayer behavior. See also: Nova Ekonomija, The Serbian Tax Administration Also Uses Artificial Intelligence, Nova Ekonomija, available at: https://novaekonomija.rs/vesti-iz-zemlje/i-poreska-uprava-srbije-koristi-vestacku-inteligenciju. In September 2024, the Ministry of Education launched the project *Development and Implementation of Software for Monitoring the Physical Development and Motor Skills of Primary and Secondary School Students* ("Zdravitas"), which is designed to process data on students' motor abilities and cross-reference them with data from the already operational e-Dnevnik system.

[4] See, for example: Aleksa Tešić, Artificial Intelligence Is Entering Every Aspect of Society| BIRN, BIRN Serbia, 2022, available at: https://birn.rs/pametna-srbija-vestacka-inteligencija/

the operational endeavors of the A 11 Initiative concerning this matter. To comprehend the legal rationale underpinning safeguards against discrimination and to evaluate the evolution of legal practices in this domain, an examination of existing literature offers a comprehensive insight into the present circumstances and identifies countries that have adopted legislative measures and mechanisms—either proactively or in response to emerging problems—to "correct" the outcomes of automated decision-making. The countries selected for this analysis are Germany, Denmark, France, Canada, and the United Kingdom. However, the emphasis is not on individual countries, but rather on specific legal themes addressed in this research:

1. Errors and correction of data and automated decisions;
2. Transparency and the right to an explanation;
3. Scope of data processing.

Through this broader perspective and analysis of available literature offering insight into various legal systems, we aim to better understand the legal logic and protective measures in place.

In the final phase, through the processing of qualitative data and an in-depth comparative legal analysis, the study seeks to present a range of legal mechanisms, measures, legislative solutions, and practices. The ultimate goal is to develop recommendations for improving the legal framework, public policies, and administrative practices, and to contribute to a deeper understanding of the severe, far-reaching, and harmful discriminatory consequences of these systems.

The overarching finding of this research is that the analyzed legal protection frameworks tend to favor machines; the prevailing impression is that legal systems are creating an enabling environment for the development of automated decision-making systems. In addition, several key conclusions can be drawn:

1. Individual protection mechanisms are available through domestic human rights frameworks, personal data protection mechanisms, and, to some extent, administrative law.
2. The Personal Data Protection Law serves as the cornerstone of individual rights protection, offering the broadest range of measures and opportunities to safeguard individuals.
3. There are relatively few laws that specifically regulate the use and development of these systems or establish rules and mechanisms for individual protection. Legislation concerning automated decision-making systems primarily focuses on systemic solutions for managing such systems, including provisions on transparency and obligations to conduct human rights impact assessments. In essence, the protection framework is fragmented, partially developed, and structurally porous.

4. Administrative law continues to serve primarily as the legal foundation for processing and developing these systems and, in some countries, more precisely defines certain individual rights, such as the right to an explanation and the right of access to information. However, within this domain, administrative law remains largely focused on managing potential harm rather than empowering individuals or, as would be preferable, establishing new forms of protection and procedures.
5. Judicial decisions addressing the protection of individual rights in specific cases remain rare. In this context, the judgment of the Hague Court concerning human rights violations arising from the use of automated decision-making systems holds particular significance (known as SyRi)[5]. The court determined that the lack of transparency in the automated system, in itself, constituted a violation of the right to privacy, without engaging in a legal analysis of the software code itself.
6. European countries are actively developing and piloting a range of automated decision-making systems. However, there remains an absence of sufficient legal mechanisms to provide meaningful and effective protection, highlighting the urgent need to develop new safeguards and revitalize existing ones—particularly within the field of administrative law—to better protect individuals.
7. Anti-discrimination principles and protective mechanisms are acknowledged in discussions of the discrimination risks posed by these systems. Nonetheless, there is limited understanding of how the broader legislative framework—not only anti-discrimination laws—can protect individuals from automated discrimination and injustice.

2. Automated Decision-Making in the Public Sector: A Brief Overview

Algorithmic decision-making in the public sector is part of a broader, earlier-initiated process of public administration "modernization." The first step in this direction was the development of e-government, followed by the digitization of previously analog-stored data.[6] These processes have primarily relied on the advancement and application of information and communication technologies (ICT). The latest (or more accurately, the penultimate) stage of this development is the introduction of an automated decision-making system with the involvement of public officials. In the final stage, these systems can independently make decisions without human intervention, as is the case with the tax fraud detection system

[5] The Hague District Court, ECLI:NL:RBDHA:2020:865

[6] C. Fisher, M. Heusberger, M. Heine, The impact of digitalization in the public sector: A systemic literature review, Schwerpunk, 2023, p.5. Digital transformation is further defined as a digitization process leading to digital institutional transformation.

developed in the Netherlands.[7] Known as the *SyRI* case,[8] this system led to the fall of the Dutch government[9] in 2021 due to administrative decisions based on discriminatory categorizations, as well as erroneous decisions derived from those categorizations and correlations. However, it is important to note that this study focuses exclusively on the penultimate stage of the "advancement and modernization" of public administration—specifically, the use of semi- or quasi-automated decision-making systems in the public sector, which operate according to '*if this then that*' logic,[10] and do not involve the application of artificial intelligence systems for these purposes.

In most Western Balkan countries, these projects are typically implemented as part of public administration reform processes, often with the support of international donors and the involvement of domestic or foreign private companies.[11] This public-private collaboration raises a range of issues, including the transparency of contracts and their subject matter (for example, software code), oversight and transparency in the development of software solutions, and questions of liability for system errors. Ultimately, as partnerships between the public and corporate sectors strengthen, so does their mutually reinforcing power, counterbalanced only by citizens, the media, and the courts.[12]

Setting aside this power dynamic, it is important to note that decisions regarding the development of these systems—such as the selection of companies, the areas of public administration to be automated, and the potential human rights impacts—are rarely the subject of public or expert debate. Much like the algorithmic "black boxes," the development process of these systems, which make decisions with life-altering consequences for individuals, is

---

[7] Appelman, N., Fahy, R. & van Hoboken, J., Social Welfare, Risk Profiling and Fundamental Rights: The Case of SyRI in the Netherlands, 2021, available at: https://www.ivir.nl/publications/social-welfare-risk-profiling-and-fundamental-rights-the-case-of-syri-in-the-netherlands

[8] See also: Van Bekkum, M, Zuiderveen Borgesius, F, Digital welfare fraud detection and the Dutch SyRI judgment, 2021, available at: https://journals.sagepub.com/doi/pdf/10.1177/13882627211031257

[9] See: BBC, Dutch Rutte government resigns over child welfare fraud scandal, 2021, available at: https://www.bbc.com/news/world-europe-55674146

[10] A. Huggins, Addressing Disconnection: Automated Decision Making, Administrative Law, and Regulatory Reform, UNSW Law Journal, Volume 44(3), 2021, p.1060, see also: H. C. H. Hoffmann, Automated Decision Making (ADM) in EU Public Law, Law Research Paper Series. No.2023-06, Indigo,2023

[11] See also: SERBIA - Interoperable Europe, available at: https://interoperable-europe.ec.europa.eu/sites/default/files/inline-files/NIFO_2024%20Supporting%20Document_Serbia_vFINAL.pdf, NiFO, 2024 and World Bank and Digitalization, World Bank, n-d, available at: https://projects.worldbank.org/en/projects-operations/project-detail/P174555. See also: https://www.ite.gov.rs/vest/sr/4199/kancelarija-za-it-i-eupravu-i-svetska-banka-zajedno-do-sveobuhvatne-digitalizacije-usluga-javne-uprave-za-gradjane-i-privredu.php

[12] B. Kostić, Uncontrolled Surveillance, Uncontrolled Consequences: A Brief Overview of the Impact on Freedom of Expression and Media Freedom, OSCE Serbia, 2022

shrouded in secrecy—and even *mystique*. This mystique has been fueled by political narratives promising far-reaching positive outcomes from automated public administration. It is therefore not uncommon for these systems to be described as faster, more efficient, more transparent, more participatory, and less prone to error thanks to their computerized logic. Advocates also claim that they reduce public administration costs and corruption risks,[13] and overall, are "better" for citizens by facilitating access to services and rights.[14] This instrumental and utilitarian approach to public administration has only been intensified and accelerated by processes of automation and digital transformation. Often, it neglects the core role of public administration and the fundamental principles of good governance—such as legal certainty, openness and transparency, participation, accountability, and others—enshrined in numerous international and national instruments.[15]

Numerous cases worldwide illustrate this trend. For example, in Germany, approximately 25% of individuals' tax statements are processed automatically, with this proportion increasing each year.[16] In Denmark, the *Gladsaxe* system was developed for municipal use with the aim of monitoring children in vulnerable situations before they might be categorized as having special needs, using criteria such as mental health issues, unemployment, or missed dental appointments. Municipalities participating in the pilot project requested exemptions from data protection rules. Following public outcry, the project was ultimately not implemented. However, Denmark has automated a significant portion of its social welfare system. For instance, in the quest to identify social benefits fraud, the authorities deploy the Really Single algorithm in an

[13]C. Fisher, M. Heusberger, M. Heine, The impact of digitalization in the public sector: A systematic literature review, Schwerpunk, 2023, p.4,5. See also: M. Choroszewicz and B. Maihaniemi, Developing Digital Welfare State: Data Protection and the use of Automated Decision Making in the Public Sector across Six EU Countries, University of California Press, Global Perspectives, 2020, p.2

[14] These objectives are indirectly defined in the Social Card Law, Article 3 ("Official Gazette of the RS", No. 14/2021). The aim of establishing the Social Card system is to create a unified and centralized electronic registry containing accurate and up-to-date information on the socio-economic status of individuals and related persons. This registry enables data users to process information necessary to determine facts required for exercising rights and accessing services in the field of social protection. Specifically, it aims to facilitate more efficient access to social protection rights and services, ensure a fairer distribution of social assistance, improve the efficiency and proactivity of authorities working in the area of social protection, support the development and shaping of social policy, monitor the overall effects of social protection measures, and provide updated information on beneficiaries in case of emergency situations.

[15] See also: Public Administration Reform Strategy in the Republic of Serbia for the period 2021–2030, "Official Gazette of the RS", No. 42/2021, 9/2022.

[16] Developing Digital Welfare State: Data Protection and the Use of Automated Decision Making in the Public Sector across Six EU Countries, p.8.

attempt to predict a person's family or relationship status.[17] It is worth noting that Denmark was cited by officials in Serbia as a model for developing the Social Card system.[18]

Similar systems have been developed in other European Union countries.[19] There is an observable trend toward creating automated decision-making systems that, on the one hand, aim to improve the efficiency of monitoring cases of tax evasion and fraud, and, on the other, seek to reduce errors and abuses within social protection systems. To date, research has not indicated that similar systems are used to monitor or control financially well-off citizens.

The definition of automated decision-making systems (ADM), frequently cited in academic literature, refers to systems, software, or processes designed to assist or replace humans in decision-making.[20] These systems—such as the Social Card system—involve the interaction of various automated systems, databases, and human input. As a result, it is often difficult to draw a clear distinction between the roles of humans and machines. It is certain, however, that these systems *de facto* and *de jure* limit human discretion in later stages of the decision-making process.[21] Moreover, they contribute to the problem of so-called "automation bias," where an official's discretionary decision is influenced by automated systems. **These systems do not merely inform public officials; rather, they typically "shape, constrain, and even remove"[22] human involvement from critical phases of decision-making, due to the "way they categorize information and construct profiles of individuals."**

In any case, the operation of these systems requires vast amounts of data, which have been converted from analog formats into computer-readable language as part of the previously mentioned digitization process. Once digitized, this data—through the development of large-

---

[17] See also: Hellen Mukiri-Smith, Hajira Maryam, and David Nolan, Amnesty Tech How We Did It: Amnesty International's Investigation of Algorithms in Denmark's Welfare System – Global Investigative Journalism Network, 2024, available at: https://gijn.org/stories/amnesty-internationals-investigation-algorithms-denmarks-welfare-system/ as well as in the report by Amnesty International, Coded Injustice - Surveillance and Discrimination in Denmark's Automated Welfare State, Amnesty International, 2024, available at: https://www.amnesty.org/en/documents/eur18/8709/2024/en/

[18] Minister Đorđević and the Danish Ambassador, Horgaard, on the Introduction of Social Cards in Serbia, Ministry of Labor, Employment, Veteran and Social Affairs, 2018, available at: https://www.minrzs.gov.rs/sr/aktuelnosti/vesti/ministar-djordjevic-i-ambasador-danske-hogard-o-uvodjenju-socijalnih-karata-u-srbiji

[19] The Algorithmic watch, The Algorithmic administration, n-d, available at: https://algorithmwatch.org/en/algorithmic-administration-explained/

[20] Rashida Richardson, Confronting Black Boxes: A Shadow Report of the New York City Automated Decision System Task Force, AI Now Institute, 2019, p. 6, available at: https://ainowinstitute.org/ads-shadowreport-2019.pdf

[21] "The use of ADM technologies could therefore *de facto* or *de jure* limit discretion of a human decision-maker in a later phase of a decision-making procedure," C. H. Hoffmann, Automated Decision Making (ADM) in EU Public Law, Law Research Paper Series. No.2023-06, Indigo, 2023.

[22] Automated Decision Making (ADM) in EU Public Law, p.20

scale information systems, their interconnection, and interoperability[23] —becomes the foundation for automated decision-making systems. The data processing and cross-referencing primarily involve already available *derived* or *inferred* data. Derived data might include, for example, determining an individual's citizenship based on a certificate of nationality, while inferred data could involve estimating an individual's health status based on processed health information.

In addition to the challenges already mentioned, issues can also arise from the data themselves. Beyond the risk of inaccuracies, data are often incomplete or insufficiently representative. Automated systems built on such data can become rife with errors, discrimination, and oversimplification.

The first step in developing automated systems is data mining, and even at this early stage at least three ways in which the process can foster discrimination have been identified. First, there may be a deliberate effort to disadvantage members of certain protected groups in ways that are difficult to detect. Second, the data mining process itself can introduce errors, reflecting underlying biases and inaccuracies that disproportionately affect specific social groups. Third, unintended consequences of data mining can shape decision-makers' judgment, potentially reinforcing social inequalities—even when no explicit errors or negligence are present.[24]

As noted, these systems do not necessarily exclude human involvement, nor would such exclusion be desirable. The *human in the loop* concept underscores the corrective and supervisory role of humans throughout the process—from system development and deployment to oversight and accountability for individual decisions. In this process, one or more individuals perform a supervisory role, receiving information and influencing the operation of an otherwise closed and autonomous system.[25] However, this does not mean that these systems are incapable of producing outcomes—such as decisions—without the involvement of public officials. On the contrary, they can, especially when powered by AI and machine learning. As will be discussed further, the SyRI system in the Netherlands and a similar system developed in Denmark,[26] are examples of such cases. The Social Card system currently operates as a semi- or quasi-automated system, at least based on the information available. Like many similar systems, it is not accessible to the public. In Germany and France, independent human rights bodies have recommended that the computer code—that is, the

[23] *Ibid*.

[24] S. Barocas, Data Mining and the Discourse on Discrimination. Proceedings of the Data Ethics Workshop, Conference on Knowledge Discovery and Data Mining (KDD), 2014, p.3

[25] Iyad Rahwan, Society-in-the-Loop: Programming the Algorithmic Social Contract, Ethics and Information Technology, 20(1), 201, p.6.

[26] Amnesty International, Coded Injustice - Surveillance and Discrimination in Denmark's Automated Welfare State, 2024.

logic underlying the system—be made available to the public.[27] When this occurred in Rotterdam, it was revealed that the algorithm used to detect fraud in the social welfare system discriminated against beneficiaries based on gender and ethnic origin, offering the public a clear example of how harmful such systems can be.[28]

Serbia

All of the experiences described above indicate that such systems, as a rule, tend to automate problems that disproportionately affect the most vulnerable segments of society, particularly individuals living at or near the poverty line. According to UNICEF estimates for 2023, approximately 800,000 people in Serbia were living in absolute poverty, while around 1.3 million were at risk of poverty.[29] It was in this context—and amid a wave of techno-optimism—that Serbia adopted the Social Card Law.[30] The law was enacted in February 2021, at the height of the COVID-19 pandemic, more than 18 months after the conclusion of a public consultation during which various stakeholders, including independent bodies, provided predominantly critical feedback on the draft legislation. Among these were the Commissioner for the Protection of Equality and the Commissioner for Access to Information of Public Importance and Personal Data Protection. The latter, among other concerns, noted that the data processing impact assessment required under the draft law did not meet the standards set by the Law on Personal Data Protection (LPDP).[31]

Article 3 of the Social Card Law states that the purpose of the legislation is to establish a unified and centralized registry of the socio-economic status of individuals and their associated persons. This would enable administrative authorities responsible for decision-making within the social protection system to better process data in order to establish the facts necessary for exercising rights and accessing services in the field of social protection. These efforts are undertaken to improve efficiency, ensure a fairer distribution of social benefits, enhance the proactivity of administrative authorities responsible for social protection, provide support for

[27] Developing Digital Welfare State: Data Protection and the Use of Automated Decision Making in the Public Sector Across Six EU Countries, p.6

[28] See: Wired, Inside a Misfiring Government Data Machine, 2023, Wired, available at: https://www.wired.com/story/algorithmic-bias-government/

[29] Gojko Vlaović, 1.3 Million People at Risk of Poverty in Serbia, NIN, 2024, available at: https://www.nin.rs/drustvo/vesti/59949/u-riziku-od-siromastva-u-srbiji-13-miliona-ljudi

[30] "Official Gazette of RS" no. 14/2021.

[31] D. Ćurčić, Privacy and Data Protection in Serbia – An Analysis of Selected Sectoral Regulations and Their Implementation, Partners for Democratic Change Serbia, 2021, p. 58, available at: Privatnost_i_zaštita_podataka_o_ličnosti_u_Srbiji-_Analiza_odabranih_sektorskih_propisa_i_njihove_primene.pdf

defining and shaping social policy, monitor the overall effects of social protection measures, and provide updated information on beneficiaries in case of an emergency. [32]

Although the law does not explicitly mention the use of algorithms, it identifies the automation of procedures and processes related to social protection as one of the purposes of data processing within the Social Card system.[33] However, it is unclear what is meant by "procedures" and "processes"—specifically, whether they refer to administrative proceedings, in which case the system would constitute automated decision-making. A textual interpretation of this provision suggests that the legislature intended automation to move beyond quasi-automated data processing toward full automated decision-making. Nonetheless, despite this intent—and despite the fact that the law's 25 articles have, in the first two years of implementation, resulted in around 58,000 beneficiaries losing access to social assistance,[34] — there is little mention of mechanisms to protect individual rights or of additional opportunities to challenge decisions. The following section, therefore, examines key legal issues and comparative experiences related to the protection of individual rights in procedures that involve, fully or partially, automated decision-making in the public sector.

3. General Legal Considerations

In relation to the protection of individual rights in such procedures, the literature reviewed for this research emphasizes the intersection of three legal domains that regulate and govern automated decision-making systems. These include: the general framework for the protection of human rights, encompassing the right to equality and protection from discrimination;[35] the framework for personal data protection and information security; and the provisions of administrative law, including those regulating administrative procedures.

The fundamental legal framework for the protection of human rights and freedoms is established by all major international instruments,[36] most of which have been ratified by Serbia and codified in its Constitution. Regarding legislative solutions based on human rights-based approach in the context of new technologies, recently adopted acts of the European Union and

[32] *Ibid,* p. 56.

[33] Social Card Law, Artic 4. 1(4).

[34] A 11 Initiative, Information received from the Ministry of Labour, Employment, Veteran and Social Affairs, https://antisocijalnekarte.org/

[35] J. Niklas, Human Rights Based Approach to AI and Algorithms, in The Law of Algorithms, ed. by W. Barfield, Cambridge University Press, 2020, p.24

[36] Such as the Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights, the European Convention on Human Rights, and the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, including its Additional Protocols.

the Council of Europe are particularly significant. In May of this year, the European Parliament and the Council adopted the Regulation laying down harmonized rules on Artificial Intelligence (the Artificial Intelligence Act) amending certain Union legislative acts.[37] The Artificial Intelligence Act aims to establish obligations for those who develop, implement, and use AI in relation to specific applications of the technology and classifies AI systems according to the severity of risks they pose to human rights and freedoms. Perhaps the most significant step to date in setting international standards for the development and use of artificial intelligence is the recently adopted Council of Europe Framework Convention on Artificial Intelligence, Human Rights, Democracy and the Rule of Law.[38] This Framework Convention is notable as it represents the first binding international instrument defining the core principles and standards that signatories must uphold throughout the entire lifecycle of AI applied by public authorities or private entities acting on behalf of public authorities.

Furthermore, the legal frameworks for the protection of personal data and privacy—particularly with regard to information privacy and information security—play a crucial role in enabling individuals to exercise specific rights, such as the right of access and erasure, and even, under certain conditions, to refuse to be subject to automated processing. In addition, data protection principles are essential, as they establish standards of transparency and the right to explanation, which data controllers are obligated to uphold. In this regard, the most important legal instrument is certainly the EU General Data Protection Regulation (GDPR),[39] which serves as a key source of law for both automated and non-automated data processing. The Law on Personal Data Protection of the Republic of Serbia was adopted following the model of the GDPR.[40] Although the GDPR harmonizes the law and applies directly in EU Member States, it also allows Member States to adapt certain provisions to their legal systems or derogate from specific provisions under the conditions set out in Article 23 of the GDPR. Several EU countries have either derogated from or otherwise regulated automated decision-making and, by doing so, may have implicitly limited certain data protection rights (this will be discussed in more detail below). In cases where certain GDPR provisions were derogated during transposition

[37] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonized 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), OJ L, 2024/1689, 12 July 2024.

[38] Council of Europe Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law, available at: https://rm.coe.int/1680afae3c

[39] Regulation (EU) 2016/679 of the European Parliament and of the Council 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, and repealing Directive 95/46/EC (General Data Protection Regulation), available at: https://eur-lex.europa.eu/eli/reg/2016/679/oj

[40] "Official Gazette of RS," no. 87/2018.

into national legislation, countries have introduced various alternative protection mechanisms, such as the right to access information.[41]

In addition to the above, administrative law provisions are also an important source of protection for citizens. However, they remain insufficiently updated to adequately address issues related to the status of individuals and the protection of their rights in the context of automated decision-making.[42]

The following discussion focuses on legally binding statutory frameworks ("hard law"), setting aside various by-laws and national strategies which, particularly in Serbia, have often embraced techno-optimism and set high expectations for these systems, frequently at the expense of protecting human rights and freedoms. Regardless of the specific legal field, the core issue remains the same: who controls technological processes? Put differently, "**how does a legal system govern the interface between the automated part of a decision-making procedure and the human input into decision-making?"**[43] Any legal response to this question must align the logic of computing systems with the legal language of the domestic legislative framework[44] - a complex and demanding task.

From a legal standpoint, automated systems give rise to a distinct form of administrative decision-making. Data retrieved from one or more databases is cross-referenced through various algorithmic correlations, sometimes to calculate probabilities,[45] such as the likelihood of reoffending, as in the COMPAS system used in the United States,[46] or more generally, to assess eligibility for certain rights, as in the case of the Social Card system. In both cases, the software underpinning automated decision-making supports the issuance of executive decisions by identifying criteria and procedures that, in effect, prepare the ground for individual decisions. These decisions may be a direct or indirect result of applying the software. In this sense, software can influence both rule-making and decision-making procedures."[47]

---

[41] Developing Digital Welfare State: Data Protection and the use of Automated Decision Making in the Public Sector across Six EU Countries, p.18.

[42] Addressing Disconnection: Automated Decision Making, Administrative Law, and Regulatory Reform, p.1071, L. Edwards et al., Legal and regulatory frameworks governing the use of automated decision making and assisted decision making by public sector bodies, Workshop briefing paper, The Legal Education Foundation, 2021, p.31.

[43] Automated Decision Making (ADM) in EU Public Law, p.16, 35.

[44] Addressing Disconnection: Automated Decision Making, Administrative Law, and Regulatory Reform, p. 1052.

[45] Automated Decision Making (ADM) in EU Public Law, p. 3, 6.

[46] Jeff Larson, Surya Mattu, Lauren Kirchner and Julia Angwin, How We Analyzed the COMPAS Recidivism Algorithm, Propublica, 2016, available at: https://www.propublica.org/article/how-we-analyzed-the-compas-recidivism-algorithm.

[47] Automated Decision Making (ADM) in EU Public Law, p. 6.

Despite the transformative impact of software on the method and process of decision-making regarding citizens' rights in administrative procedures—and beyond— the underlying code is rarely subject to legal regulation, either at the EU level or within national jurisdictions. This regulatory gap extends both to systemic rules governing the use and development of these systems and to the issuance of individual decisions and the influence of systemic solutions on such decisions.[48] Some legal perspectives argue that the law should primarily and fundamentally focus on the organization and procedures of decision-making, rather than on the algorithms themselves. In other words, "public administrations, rather than machines, remain legally responsible for any decision made through automated processing."[49]

The Court of Justice of the European Union (CJEU) has ruled that the use of such systems must be preceded by established models and criteria for their intended use, which must be grounded in the legal framework—in other words, there must be a valid legal basis.[50] In the same ruling, the Court noted that any automated decision based on models or connection criteria rooted in racial, religious, ethnic, or other types of data, including those related to gender and health, may adversely affect the rights to privacy and data protection. **The Court thus clearly holds that these systems carry high risks of discrimination, primarily because they process data to categorize individuals based on similar statuses (for example, vehicle ownership) and characteristics (such as age), and then make decisions based on these distinctions. These decisions may rely not only on inaccurate data but may also be inherently legally impermissible and discriminatory.**[51] This position has also been affirmed by the provisions of the AI Act, which classifies among prohibited artificial intelligence systems those that perform so-called social scoring, precisely because of their discriminatory nature.[52]

In Serbia, this applies specifically to the Social Card Law. As mentioned, this Law does not explicitly mandate the use of algorithms or automated decision-making within the social protection system. However, it does provide for the automation of procedures and processes related to actions in the field of social protection. Neither the text of the Law nor the (limited and contradictory) data available to the public make it entirely clear which parts of the procedures are automated. Understanding the relationship between automated data processing and human involvement is further complicated by the fact that neither the source code nor the underlying algorithmic logic has been made available to the public—including the expert community.

---

[48] *Ibid*, p.7.

[49] J. Cobbe, Administrative Law and Machine Learning Judicial Review of Automated Public Sector Decision Making, Cambridge University Press, 2019, p.6.

[50] CJEU Ruling, 6 October 2020,C-511-520/18 La Quadrature du Net ECLI:EU:C:2020:791, para 181.

[51] Automated Decision Making (ADM) in EU Public Law, p. 31.

[52] Article 5. 1. (c) and Recital 31 AI Act.

Compliance of Data Processing in the Social Card System with the Law on Personal Data Protection

From the perspective of personal data protection—which, in comparative practice, is the most common basis for assessing the lawfulness of such systems and the adequacy of rights protection mechanisms—it is evident that the Social Card Law is not aligned with the overarching Law on Personal Data Protection. This conclusion holds true regardless of the role of automated data processing in the decision-making process.

Specifically, the provisions of the Social Card Law violate several key principles of personal data protection, including:

- **The principle of data minimization** requires that processed data be adequate, relevant, and limited to what is necessary for the purpose of processing.[53] However, the Social Card Law permits the processing of 135 sets of data about individuals who are either beneficiaries of social protection rights and services or applicants for such rights. "The scope of personal data processed under this system is without precedent in any other context within the Republic of Serbia and represents an excessive degree of data processing with respect to recipients of financial social assistance and other individuals applying for entitlements within the social protection system."[54] Establishing such a system requires conducting a necessity test, whereby the public administration must demonstrate that the data processing is permissible, purposeful, and that no less invasive means of achieving the same objective exist.[55] Judging by the text of the Social Card Law and the data protection impact assessment conducted during the legislative drafting phase, no such test was carried out either when establishing the legal basis or when developing the Social Card system itself.

- **The purpose limitation principle** stipulates that personal data must be collected for specific, explicit, justified, and lawful purposes and must not be further processed in a manner incompatible with those purposes.[56] Although the Social Card Law refers to this principle57, and, in Article 4, sets out the purposes of data processing, it does not specify which of the 135 data points are processed for each particular purpose. As a result, the purposes of processing are neither defined nor explicit. Subsequently

[53] Article 5, paragraph 1, item 3 of the Law on Personal Data Protection.

[54] Initiative to Launch a Procedure for Constitutional and Legal Review of the Social Card Law, A 11 - Initiative for Economic and Social Rights.

[55] J. Cobbe, Administrative Law and Machine Learning Judicial Review of Automated Public Sector Decision Making, Cambridge University Press, 2019, p.11.

[56] Article 5, paragraph 1, item 2 of the Law on Personal Data Protection.

[57] Article 18, paragraph 2 of the Social Card Law.

adopted by-laws (Rulebooks) specify the content of the forms used, but the level of predictability regarding the purpose, type, and scope of data should be established by law, not by secondary legislation, as required by Article 14 of the Law on Personal Data Protection. Among other things, the Social Card Law does not prescribe measures to ensure the lawful and fair processing of data, but merely makes a declarative reference to the application of regulations in the field of personal data protection.

- The principle of lawfulness, fairness, and transparency of data processing requires that data be handled in a lawful, fair, and transparent manner in relation to the data subject. This principle is further elaborated by the provisions of the Law on Personal Data Protection (LPDP), which impose an obligation on data controllers to inform data subjects of all relevant aspects of the processing, as well as of the mechanisms available to exercise their rights. The LPDP does allow for certain limitations to the right to information when data are not collected directly from the data subject. One such exception applies when the collection or disclosure of data is explicitly prescribed by law; however, such legislation must meet specific standards - namely, it must prescribe appropriate measures for the protection of the rights, freedoms, and legitimate interests of the data subjects. The Social Card Law does not meet these requirements. Specifically, the rights established by the LPDP represent minimum standards, and the possibility of restricting these rights may only be prescribed for the protection of certain interests enumerated in Article 40 of the LPDP (the provision of social welfare services is not included among those interests). Any regulation that permits the processing of personal data not collected directly from the data subject must also establish additional safeguards to protect the rights, freedoms, and legitimate interests of the individuals concerned. Furthermore, in cases involving automated decision-making, including profiling, the LPDP imposes an additional requirement on data controllers: they are required to inform the data subject of the existence of automated decision-making and, at a minimum, provide meaningful information about the logic involved, as well as the significance and anticipated consequences of the processing for the data subject. According to available practical evidence, such information is not provided to citizens within the social protection system. However, it remains unclear whether this is due to the absence of automated decision-making or the data controller's failure to comply with this legal obligation.

Moreover, if the Social Card system employs automated individual decision-making, the Social Card Law fails to meet the required standards for legislative quality. Drawing on the model established by the GDPR (see more below), Article 38 of the LPDP provides that a data subject has the right not to be subject to a decision based solely on automated processing. However, if such a decision is based on law, this right may be restricted, provided that the law prescribes appropriate measures to protect the rights, freedoms, and legitimate interests of the data subject. Apart from referencing the LPDP and the application of regulations in the areas of

information security, electronic administration, and electronic identification, the Law does not go further in addressing the protection of individuals' rights and interests or in specifying security measures. As a result, it fails to meet the requirements for the quality of legislation as outlined in Article 38, paragraph 2, item 2 of the LPDP.

4. Primary Legal Considerations

Taking into account comparative experiences as well as the key shortcomings identified in the Social Card Law with regard to the protection of individuals' rights, this section examines systemic and legal solutions adopted in various European countries from the perspective of the following legal issues:

1. Errors and corrections of data and automated decisions;
2. Transparency of these systems and the right to an explanation;
3. The scope of data processing.

It is important to emphasize at the outset that the countries whose legislation has been analyzed—based on secondary literature—only partially regulate the issues that are the focus of this study. Moreover, there is a very limited number of legal instruments that specifically and explicitly address automated decision-making systems.[58] As already noted, the current stage of legal development highlights the importance of having a legal basis for such decisions, whether through individual or general acts, as is the case in France, for example.[59] Such a legal basis should align with the principles of *good governance*. Within this principle, the duty of due diligence underscores the importance of documenting and reporting on the sources of information (such as databases) and the computer processes and "logic" that led to the decision. Thus, the ability to verify and trace the manner in which a specific decision was made (*traceability*) is highly important.[60]

In the context of EU Member States, **Article 22 of the GDPR** is particularly significant, as it sets certain restrictions on automated decision-making. Specifically, this provision allows individuals not to be subject to a decision based solely on automated processing where such decisions produce legal effects concerning them or similarly significantly affect them. However, this rule applies only to systems that rely entirely on machine learning, thereby excluding human officials from the process.

---

[58] See: Developing Digital Welfare State: Data Protection and the use of Automated Decision Making in the Public Sector across Six EU Countries; see also: Ada Lovelace Institute, Algorithmic Accountability in the Public Sector, 2021, p.46.

[59] Developing Digital Welfare State: Data Protection and the use of Automated Decision Making in the Public Sector across Six EU Countries, p.4.

[60] Automated Decision Making (ADM) in EU Public Law, p. 23

Nonetheless, the GDPR establishes exceptions to the application of this right, including cases where the decision is necessary for entering into, or performance of, a contract, where it is based on the explicit consent of the data subject, or where it is grounded in law. In the first two cases, the individual has the right, *inter alia*, to request human intervention in a meaningful way—that is, in a manner that could change the decision.[61] However, this right is not guaranteed when the decision is based on law, but additional protection is provided through the requirement for a particular quality of legislation—such laws must prescribe appropriate measures to protect the rights, freedoms, and legitimate interests of the data subjects. These are standards and safeguards that should go beyond those provided by data protection regulations.

Such provisions on automated individual decision-making and profiling have served as a foundation for several EU Member States to establish a legal basis for automated data processing through specific legislation. In some instances, these special laws also permit the processing of sensitive data (i.e., special categories of personal data), the processing of which would otherwise be prohibited under Article 22.[62]

For example, Finland has adopted a secondary regulation that permits the *secondary* processing of health and social protection data. In addition, the country has enacted the Law on Information Management, which establishes rules that public authorities must observe in the data processing procedure. These rules are grounded in the principles of good governance and aim to promote data interoperability. In Denmark, the Public Administration Law contains provisions on technology development aligned with core administrative values. A specialized public body has also been established to facilitate data exchange and cross-referencing among public authorities through secondary processing, which is likewise permitted under the national legal framework. This body, together with a private company to which technical and administrative competencies and responsibilities have been delegated, was established by the Udbetaling Danmark Act. This Act centralized the administration of social benefits that fall under municipal jurisdiction, including child allowances, pensions, housing benefits, unemployment benefits, sickness benefits, and other forms of social assistance.[63] A report by Amnesty International from October 2024 concluded that this system creates individual risks concerning access to legal remedies, primarily due to the lack of transparency towards

[61] Article 29 Data Protection Working Party, 2018a; see also: J. Cobbe, Administrative Law and Machine Learning Judicial Review of Automated Public Sector Decision Making, Cambridge University Press, 2019, p.11.

[62] Developing Digital Welfare State: Data Protection and the Use of Automated Decision Making in the Public Sector across Six EU Countries, University of California Press, p. 3, see also: J. Cobbe, Administrative Law and Machine Learning Judicial Review of Automated Public Sector Decision Making, Cambridge University Press, 2019, p.11.

[63] Amnesty International, Coded Injustice - Surveillance and Discrimination in Denmark's Automated Welfare State, p.10, 18.

individuals whose rights are being decided upon— particularly those flagged by the algorithm as likely to commit social benefit fraud. Furthermore, the report found that the Public Administration Law does not contain provisions that mandate public authorities to inform individuals that a case against them originated from an algorithm. "Because a person is unaware that they are the subject of an automated process, they cannot effectively challenge the decisions of the UDK system."[64] Additionally, Germany has amended its Administrative Procedure Act by introducing Article 35, which generally allows for the automatic processing of data but requires further regulation through specific legislation for each particular use. Interestingly, the German Data Protection Law explicitly permits the processing of special categories of personal data, subject to the obligation to establish protective measures that are also prescribed by law. The German Social Welfare Law allows for the automatic processing of data and specifies that this law is considered *lex specialis* in relation to data protection legislation.

France adopted the Digital Republic Act along with amendments to the Administrative Law, introducing a provision on algorithmic transparency. The legislative process in France was accompanied by a period of public consultation, which was open to all citizens for three weeks and included organized expert discussions with representatives of government authorities. Additionally, the authorities committed to responding to individual proposals submitted during the public consultation process. The Law aims to advance open data policies and the knowledge economy while safeguarding privacy and personal data. It expands the powers of public authorities in handling data and official documents by introducing new legal instruments. First, existing documents and data from public administration— at both local and national levels—may be made publicly accessible, thereby reducing the time required to obtain such data, as they will be freely available online. These publicly available data can be reused—through secondary use—even "beyond the mandates of the public services for which the data were originally collected."[65] The law serves as a *lex specialis* in relation to the Data Protection Law and provides certain forms of protection, such as the right of individuals to determine how their data will be made available and used. It also strengthens rights already enshrined in the Data Protection Law, such as the right to object. The powers of the French Data Protection Authority (CNIL) have been expanded, allowing for deeper and broader involvement in open data processing activities.[66] France has also adopted a specific secondary regulation that further defines the obligations of public services, which is addressed in the following chapter.

---

[64] *Ibid.*, p.12.

[65] Digital Republic Bill, Overview and Explanatory Memorandum, Chapter I, available at: https://www.republique-numerique.fr/pages/in-english

[66] Digital Republic Bill, Overview and Explanatory Memorandum, Chapter II, Article 16-20, available at: https://www.republique-numerique.fr/pages/in-english.

Similar laws are currently under public discussion in the Netherlands (Digital Government Law[67] and the Law on Digital Data Processing through Partnerships[68]), as well as in the United Kingdom and Canada.[69] In the United Kingdom, for example, a proposed law, specifically addressing algorithmic and automated decision-making, envisions the creation of a public register of these systems. It also establishes obligations for public officials involved in making individual decisions—issues that will be further examined in the next chapter. Notably, the law requires public authorities to provide training for officials using these systems, enabling them to develop expertise in the field. Finally, the law outlines Principles for Auditability, Explainability, and Oversight of these systems. These principles are more aspirational—both legally and ethically—than strictly prescriptive or enforceable.[70]

The Canadian Law on Automated Decision-Making primarily addresses the governance of such systems and the obligations of public authorities, but it does not establish specific rights for individuals affected by these decisions. Unlike other laws, the entire regulatory framework is based on human rights systemic risk approach, categorizing risks into three levels: low, medium, and high. Each government authority using these systems is required to conduct a risk assessment and align the system's operation with the identified level of risk. The law also outlines specific measures for the correction and control of systems based on their risk classification. Furthermore, it regulates both semi-automated (quasi-automated) and fully automated systems, whose use is prohibited without human involvement. The law explicitly mandates that "the final decision must be made by a human."[71]

4.1. Errors and Corrections of Data and Automated Decisions

Every correction of errors requires highly sophisticated knowledge by officials regarding the functioning and underlying logic of these systems. The correction process should not focus

[67] Developing Digital Welfare State: Data Protection and the use of Automated Decision Making in the Public Sector across Six EU Countries, p.4, available at: https://www.nldigitalgovernment.nl/overview/legislation/ - It does not specifically address the field of automated public administration.

[68]Partnerships between various government authorities for the purpose of data processing for clearly defined, yet broadly framed purposes. The Law is expected to enter into force on January 1, 2025, available at: https://www.government.nl/latest/news/2024/06/18/senate-approves-data-processing-by-partnerships-act. Another law is currently under discussion in the Netherlands: Act Strengthening the Guarantee Function of the General Administrative Law (Awb).

[69] Directive of Automated Decision Making, Canada, 2020, Appendix C, available at: https://www.tbs-sct.canada.ca/pol/doc-eng.aspx?id=32592&section=html.

[70] Public Authority Algorithmic and Automated Decision-Making Systems Bill [HL], September 2024, available at: https://bills.parliament.uk/bills/3760/publications

[71] Directive of Automated Decision Making, Canada, 2020, Appendix C, available at: https://www.tbs-sct.canada.ca/pol/doc-eng.aspx?id=32592&section=html.

solely on addressing system- or data-related errors; rather, officials must be capable of making decisions independently of automated systems.[72] But is it realistic to expect public officials to possess such a level of digital literacy and skills? A focus group conducted as part of the project underpinning this research revealed that officials employed in centers for social work are, at best, capable of using the **Social Card system's software. However, tasks such as correcting decision-making errors, verifying the accuracy of data, and ultimately issuing a decision contrary to the system's recommendation require extraordinary effort, if they are even possible at all. The prevailing impression is that this system has further tied the hands of social workers, who are most often responsible for determining eligibility for social benefits. Crucially, this overlooks the fact that these roles are predominantly held by women, who are typically the ones in direct contact with clients and most familiar with their life circumstances.**

For individuals to be able to request a correction, they must first understand how the error occurred, which will largely define the ability to challenge the decision and provide the legal basis for an objection or appeal.[73] In this respect, the approach taken by the Law on Algorithmic and Automated Decision-Making in the United Kingdom is noteworthy. By regulating oversight mechanisms, it creates pathways for identifying and rectifying erroneous decisions. More specifically, the Law requires agencies using these systems to retain logs—that is, computerized records of system use—for a period of five years. These records must also include notes indicating whether the final decision was made in accordance with the system's recommendation. The Law even prohibits the procurement of systems that lack these capabilities, including the ability to monitor the decisions generated through such systems.[74]

In this context, the right to correct errors is closely linked to the right to an explanation, or, more broadly, to system transparency. In Serbia, it appears that the legal framework for personal data protection offers individuals more accessible and flexible mechanisms than those provided under the general rules of administrative procedure. Specifically, the Law on Personal Data Protection (Article 29) grants individuals the right to rectification and supplementation, allowing data subjects to have inaccurate personal data corrected without undue delay. Additionally, depending on the purpose of processing, the data subject has the right to supplement incomplete data, including by submitting an additional statement. However, this mechanism applies only to the rectification and supplementation of personal data processed during the procedure, whereas the Social Card system contains data that may not necessarily qualify as personal data (for example, information about real estate ownership, firearm possession, etc.). In cases of inaccuracy or outdated information of this kind (mostly

[72] Automated Decision Making (ADM) in EU Public Law, p.30.

[73] Addressing Disconnection: Automated Decision Making, Administrative Law, and Regulatory Reform, p.1066.

[74] Public Authority Algorithmic and Automated Decision-Making Systems Bill [HL], September 2024, available at: https://bills.parliament.uk/bills/3760/publications, Art. 7 and 8.

automatically generated from other public registries as prescribed by law), individuals must present evidence in administrative proceedings,[75] while the authority's ability to correct decisions is limited to obvious inaccuracies, such as errors in names, numbers, writing, or calculations. This means that, in cases of inaccurate data, the individual's primary recourse is to request the reopening of the procedure if new facts or evidence emerge.[76] However, this inevitably results in delays and prolongs the realization of their rights. Finally, with respect to the right to a legal remedy, it is worth questioning the effectiveness of such remedies in situations involving automated decision-making processes that lack transparency. **As a result, many errors that occur during the automated data processing phase— errors that influence or even determine a decision— are likely to go unnoticed by the individual (who is often a layperson) and, consequently, unlikely to be raised in an appeal.**

4.2. Algorithm Transparency and the Right to an Explanation

The issue of transparency emerged almost simultaneously with the accelerated transformation of both the public and private sectors based on the use of ICT. For example, in the context of developing AI systems, the United Nations General Assembly has emphasized that transparency, predictability, reliability, and understandability throughout the life cycle of such systems are essential for end users, including providing notice and explanation, ensuring external oversight, and enabling effective redress for individuals significantly affected by these systems—along with accountability mechanisms for those responsible for managing them.[77] Transparency must be viewed from multiple perspectives: the transparency of decisions and processes;[78] transparency toward the parties/citizens as well as public officials; and the distinction between substantive and merely formal transparency—namely, how information is made available.[79] Simply publishing the software code does not automatically satisfy the requirements for meaningful transparency. For instance, the Canadian Law on Automated Data Processing permits the publication of the software code under Article 6.2.6, except in cases where the code is classified as confidential or access is restricted under the Law on Access to Information of Public Importance.[80]

---

[75] See: Article 102 of the Law on General Administrative Procedure (LGAP).

[76] Article 176, paragraph 1, item 1 of the LGAP.

[77] UN GA, Seizing the opportunities of safe, secure and trustworthy artificial intelligence systems for sustainable development, A 78.L.49, available at: https://undocs.org/Home/Mobile?FinalSymbol=A%2F78%2FL.49&Language=E&DeviceType=Desktop&LangRequested=False, para. 6k.

[78] J. Niklas, Human Rights Based Approach to AI and Algorithms, in The Law of Algorithms, ed. by W. Barfield, Cambridge University Press, 2020, p.521.

[79] Ada Lovelace Institute, Algorithmic Accountability in the Public Sector, 2021, p.45.

[80] Directive of Automated Decision Making, available at: https://www.tbs-sct.canada.ca/pol/doc-eng.aspx?id=32592&section=html.

In practice, public administration faces two challenges. The first concerns balancing system transparency with potential associated costs and risks—such as security risks—and the practical limitations of meaningful transparency, particularly in determining what information should be disclosed and in what form. The City of Amsterdam, for example, developed a website providing an overview of a registry of AI systems used by Amsterdam's municipal authorities. This registry includes basic information about how the systems function and their intended purposes.[81] However, some authors have identified two significant shortcomings. First, the registry contains incomplete and arbitrarily selected information, offering only a limited snapshot of AI systems in use. Currently, it includes details on just four AI systems, described only in broad terms—such as automated parking control and the detection of illegal housing rentals. It omits information about systems used by the police or social services that rely on data or infrastructure from the City of Amsterdam. Moreover, it fails to indicate whether private companies have processed any of the data involved. Second, merely publishing such a registry represents only an initial step toward achieving greater transparency. On its own, it is insufficient to address the wide range of challenges associated with the use of automated systems. Moreover, the issue of transparency is closely connected to the context and political climate in which these systems are developed. The lack of contextual information prevents a proper understanding of the prevailing social, technological, and political values—or the absence thereof—that underpin AI systems. Thus, the registry ceases to serve as tools for questioning the use of AI or holding authorities accountable, especially when such systems are presented as inevitable. Instead, it becomes a tool for normalizing such systems, presenting them as benign municipal services."[82]

The draft law in the United Kingdom, which regulates the use of automated processing and algorithmic systems in the public sector, also mandates, under Article 4, the establishment of a Transparent Register of Algorithms. This register must include the following information: a description of the algorithms and automated decision-making systems, an explanation of the reasons for their application, technical specifications, details on how the use of the system affects administrative decision-making processes, and information about human oversight of these systems.[83] Furthermore, the draft law in the United Kingdom sets out detailed obligations for public authorities that use or intend to use these systems. Public bodies are required to enable the provision of meaningful and personalized explanations to individuals whose rights are being decided upon. These explanations must address the methods and reasons behind

[81] Ada Lovelace Institute, Algorithmic Accountability in the Public Sector, 2021, p.46, Amsterdam AI register, available at: https://algoritmeregister.amsterdam.nl/en/ai-register/.

[82] Corinne Cath and Fieke Jansen, "Dutch Comfort: The Limits of AI Governance through Municipal Registers," Techné: Research in Philosophy and Technology 26, no. 3 (2022), p. 395–412, available at: https://doi.org/10.5840/techne2022922125.

[83] Public Authority Algorithmic and Automated Decision-Making Systems Bill [HL], September 2024, available at: https://bills.parliament.uk/bills/3760/publications

the making of specific decisions, the decision-making process itself, and the consequences of those decisions. Authorities are also required to establish procedures for monitoring unintended consequences arising from the use of automated systems. In parallel, they must regularly verify that the data being processed are necessary, accurate, up to date, and in compliance with the Law on Data Protection. In addition, they are obliged to conduct regular audits and evaluations of the systems, including risk assessments and the adoption of measures to mitigate any identified risks.

The Importance and Legal Dimensions of Transparency: The SyRI Case

The well-known SyRI case (*System for Risk Indication*), which contributed to the fall of the Dutch government, holds particular significance as one of the rare instances that resulted in a judicial ruling. The judgment, delivered by a domestic court in The Hague, is notable for several reasons. Before outlining these, it is important to note that the Hague court, consistent with the Dutch legal system, based its decision on Article 8 of the European Convention on Human Rights—the right to respect for private and family life—following a lawsuit brought by a coalition of non-governmental organizations, which also alleged a violation of this article. This approach is a common feature of judicial proceedings in the Netherlands.

The SyRI system was developed by public administration agencies to generate risk reports identifying individuals suspected—through automated processes—of potentially breaching tax obligations. The system drew heavy criticism for disproportionately targeting low-income individuals and residents of predominantly immigrant neighborhoods across the country. In some cases, criteria such as "non-Western" characteristics (for example, surnames) were used to build the risk assessment model, drawing on data from no fewer than 17 different databases. The resulting individual risk reports flagged tens of thousands of people as potential "tax offenders." Some of those identified committed suicide,[84] and many families were left even poorer, more unstable, and more vulnerable[85]. In compliance with the court's ruling, the state paid uniform compensation to all individuals listed in the registry, regardless of the degree of intersectional injustice they had experienced. Following the judgment, and pursuant to the court's order, the system was discontinued—although this does not preclude the development of new or similar systems.

The ruling is particularly important and unique for several reasons. First, the court found that the **SyRI system constituted a legal instrument** developed by the Dutch government to

[84] Melissa Heikkila, Dutch scandal serves as a warning for Europe over risks of using algorithms, Politico, 2022, available at: https://www.politico.eu/article/dutch-scandal-serves-as-a-warning-for-europe-over-risks-of-using-algorithms.

[85] *Ibid.*

prevent and combat potential tax and social security fraud, involving local, regional, and national authorities. Once a report designated an individual as high-risk, the case was transferred to the Ministry of Social Affairs. Second, transparency was central to the court's reasoning. Invoking Article 8 of the European Convention, the court determined that information regarding the SyRI system and its underlying logic was inaccessible. The court specifically underscored that the absence of data on the risk assessments, the models used to create them, and the personal data processed—**even taking into account the information made available by the state during the proceedings**—prevented the court from verifying the parties' claims. Accordingly, the court concluded that the lack of, or insufficient, transparency of the system—combined with what it termed the "secrecy of the state"—was a key reason for finding that the SyRI system violated Article 8. Notably, at no point did the court examine the system's technical characteristics. The system was viewed primarily as a legal construct, which was particularly important given the judiciary's generally limited technical expertise in this area. In essence, **the system's code itself was not subject to legal analysis—but its lack of transparency was.**

Third, the court then proceeded to assess whether SyRI had been used in accordance with the law, as well as to examine issues of necessity and proportionality. Rather than conducting a detailed assessment of whether a clear legal basis existed, the court reframed the issue as one of "necessity in a democratic society." Once again, the court returned to the question of transparency. Citing Article 5 of the GDPR, the court found that the absence of information—even basic details—about the risk assessment process (the "decision tree") and the specific steps used to calculate individual risk scores significantly impeded individuals from participating in the process or asserting their rights. The court ordered the government to inform individuals of all key elements of the system, how these factors had influenced decisions, the contents of their individual reports and assessed risk levels, and the possibility to object to data processing with which they did not agree. The court further stated that "due to the lack of verifiable information, it is not possible to determine whether the risk of discrimination has been sufficiently mitigated," adding that this "could, for example, be achieved by making the code publicly accessible for analysis [...]."[86]

Fourth, the court specifically addressed the issue of oversight authority over the operation of the system and the correction of harm. It found that the special body established to manage the system held only an advisory role, that its recommendations were not legally binding, and that its members were, in fact, drawn from authorities with an interest in combating tax fraud. As a result, the lack of independent oversight—capable of assessing whether the large-scale cross-referencing of data was proportionate to such a narrowly defined purpose—along with an insufficiently rigorous risk assessment, were also identified as grounds for finding a violation of Article 8(2) of the European Convention, particularly concerning the principles of purpose

[86] Appelman, N., Fahy, R. & van Hoboken, J., Social Welfare, Risk Profiling and Fundamental Rights: The Case of SyRI in the Netherlands, 2021, p.16.

limitation and data minimization.[87] In this way, the Hague Court created an opening for the examination of "black box" systems like SyRI through the lens of **meaningful transparency** and institutional and administrative accountability—an approach of particular relevance from Serbia's perspective.

As the Hague Court also emphasized, the obligation of transparency for such systems is closely linked to the principle of the right to an explanation of decisions, also referred to as the "transparency of reasons".[88] In such cases, the explanation of a decision must be twofold: it must clarify how the decision was made and why?[89] Accordingly, **the rationale must be articulated and substantiated in a manner that goes beyond the traditional standards of good governance**. In fact, the complete explanation must provide information on the data that were considered and processed and "how that information influenced the final decision." Such reasoning must give the individual whose rights are at stake sufficient understanding of the factors that led to the decision, enabling them to advocate for and defend their rights as effectively as possible.[90]

The French Law on Administrative Procedure includes a provision[91] requiring public authorities to inform individuals of the extent to which algorithmic decision-making influenced an administrative decision, along with the criteria and models used by the computer program. "Although this provision initially offered hope, early experiences have not been particularly positive."[92] A secondary regulation, adopted to govern the rights of individuals subject to administrative decisions based on algorithmic processing, goes further by requiring public authorities—beyond simply providing notification—to disclose the following information upon request: **i. the degree of algorithmic data processing and how the system influenced the decision-making process; ii. the data that were processed and the sources of that data; iii. the processing parameters and how these parameters affected the specific case; and iv. the processes used in the data processing.**[93]

---

[87] *Ibid*.

[88] L. Edwards et al., Legal and regulatory frameworks governing the use of automated decision making and assisted decision making by public sector bodies Workshop briefing paper, The Legal Education Foundation, 2021, p.35.

[89] J. Cobbe, Administrative Law and Machine Learning Judicial Review of Automated Public Sector Decision Making, Cambridge University Press, 2019, p.22.

[90] Automated Decision Making (ADM) in EU Public Law, p.24

[91] Article L.311-3-1 of the 2016 Code des relations entre le public et l'administration.

[92] Automated Decision Making (ADM) in EU Public Law, p.24.

[93] Décret n° 2017-330 du 14 mars 2017 relatif aux droits des personnes faisant l'objet de décisions individuelles prises sur le fondement d'un traitement algorithmique, available at: https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000034194929.

The Canadian Law has gone even further by setting out clear requirements for explanations, tailored to the level of human rights risk for the individuals whose rights are being decided. In low-risk cases, the explanation must include elements such as: the influence of the automated system on the decision-making process; the data used; the source and method of data collection; the processing criteria and other operations; additional output information generated by the system that is relevant to the decision; and the key factors behind the decision. For medium- and high-risk systems, the explanation must also include: the exact personal data and their sources used in developing the automated processing system; the criteria applied in the specific case; other factors relevant to the decision-making analysis; and any other information that influenced the decision. The language used must be simple and clear. [94]

In the context of the Social Card system, transparency is currently ensured only through the rights provided under personal data protection law and the procedural rights of parties in administrative proceedings. The first set of rights is intended to provide transparency regarding the algorithm and its logic, while the second set is designed to ensure transparency of the decision-making process itself. However, despite these provisions, parties to the proceedings do not have access to information concerning the role (and influence) of the algorithm in the decision-making process. Therefore, it can be concluded that additional obligations for public authorities should be introduced—either through the Social Card Law or through other regulations governing the use of algorithms in public sector decision-making.

4.3. Data Processing: Scope and Purpose Alignment

The GDPR, and following its example, Serbia's Law on Personal Data Protection, establishes a range of rights for individuals whose personal data are processed, as well as various (and sometimes parallel) mechanisms for protecting these rights. These rights include: the right of access (Article 15 GDPR), the right to rectification (Article 16), the right to erasure (Article 17), the right to object (Article 21 GDPR), and the right to restriction of processing (Article 18 GDPR).

Some authors argue that these rights are inherently limited for several reasons. Although they are intended to empower individuals to exercise control over data processing—or to set boundaries on the processing of their data by controllers—when data are processed by public authorities, an inherent imbalance exists between the parties. As a result, an individual's ability to meaningfully influence the application of the principle of purpose limitation—which requires that data be processed in a legitimate, explicit, and clearly defined manner, relative to the purpose for which processing is carried out—is constrained.

An additional challenge arises in the context of secondary data use—that is, the processing of data for purposes other than those for which it was originally collected. This is particularly the

[94] Directive of the Automated Decision Making, Canada, Appendix C.

case with automated decision-making systems, which are fundamentally based on secondary data processing. The legal basis for such processing can be found in the Social Card Law and the Law on General Administrative Procedure, both of which authorize public authorities, in accordance with the law, to review, obtain, and process data from official records containing facts necessary for decision-making.[95] Nevertheless, the question remains as to how an individual can effectively exercise the rights guaranteed under the Law on Personal Data Protection.[96] When determining whether such secondary processing is permissible, both the GDPR and Serbia's Law on Personal Data Protection require the controller to assess the compatibility of the new purpose with the original one. This assessment must take into account the following factors: i) whether there is a connection between the original purpose for which the data were collected and the new purpose of the intended processing; ii) the circumstances under which the data were collected, including the relationship between the controller and the data subject; iii) the nature of the data—especially whether special categories of personal data or data relating to criminal convictions and offenses are being processed; iv) the possible consequences of further processing for the data subject; and; v) the implementation of appropriate safeguards, such as encryption and pseudonymization.[97]

As noted in the section on General Legal Considerations, the German Law on Social Protection explicitly permits the automated processing of data and the rendering of individual decisions. This Law also establishes principles of purpose limitation, prohibits the processing of data that does not comply with the frameworks set out in the Law, and mandates transparency for such systems.

Although the **Social Card Law** similarly prescribes the principles of data minimization and purpose limitation,[98] it remains questionable whether this legislation fully meets the requirements imposed on data controllers by the **Law on Personal Data Protection**, particularly with regard to assessing the potential consequences for the data subject. Equally uncertain is the extent to which individuals can invoke mechanisms under the Law on Personal Data Protection to assert a violation of the purpose limitation principle—especially when the purpose, though arguably inconsistent with that Law, is prescribed by law and therefore not subject to review in the course of individual decision-making. A more reliable—at least in terms of outcomes—legal pathway for addressing this inconsistency would be to challenge the constitutionality and legality of the **Social Card Law** itself. Unfortunately, that process remains without a legal resolution.

---

[95] Article 9(3) of the Law on Administrative Procedure.

[96] Developing Digital Welfare State: Data Protection and the use of Automated Decision Making in the Public Sector across Six EU Countries, p. 3.

[97] Article 6(2) of the Law on Personal Data Protection; Article 6(4) of GDPR.

[98] Article 18 of the Social Card Law.

5. Conclusion and Recommendations

"Behind every theory of administrative law there lies a theory of the state"
Carol Harlow and Richard Rawlings

The diverse legal approaches adopted by various countries to regulate the automated processing of data represent, albeit awkwardly, attempts to resolve the tension between automation and public law. In all cases, however, they largely reflect each country's legal traditions and broader context. In the Nordic countries, for example, general data protection regulations combined with a largely unregulated field of automated data processing are based on an underlying trust between citizens and public administration. This trust assumes that the state, acting in accordance with the principles of the rule of law and good governance, will not infringe upon citizens' rights in an impermissible manner. Yet, experience suggests that even in countries like Denmark, this trust is not always justified. In contrast, countries whose legal traditions more closely resemble Serbia's—such as Germany and France—have adopted specific laws or secondary legislation to regulate the sectoral application of such systems. For citizens, particularly those from vulnerable groups, this can result in a legal nightmare and a maze[99] where meaningful protection is achievable only if the individual possesses both legal and technical knowledge and is willing to actively defend their rights. This sets an unrealistically high bar for digital and legal literacy—one that is unattainable for many vulnerable individuals, given their social and economic conditions.

Moreover, in all countries, the legislative frameworks governing personal data protection remain inadequate to address the full range of legal challenges or to sufficiently safeguard the human rights of vulnerable groups. This is particularly true given the statutory provisions that derogate from, or create exceptions to, data protection in specific instances involving automated data processing.[100] Such legal frameworks are porous, difficult to apply at the individual level, and ultimately reinforce the power of the state. They place new burdens on individuals attempting to exercise their rights, often by introducing additional obligations or sanctions. In this legal and technological maze, a *"digital poorhouse"*[101], —a term that aptly captures the position of vulnerable groups—has emerged.

---

[99] In the literature, this issue is referred to as "intrinsic opacity", closely related to "illiterate opacity" J. Cobbe, Administrative Law and Machine Learning Judicial Review of Automated Public Sector Decision Making, Cambridge University Press, 2019, p.5.

[100] Developing Digital Welfare State: Data Protection and the use of Automated Decision Making in the Public Sector across Six EU Countries, p.10; see also Automated Decision Making (ADM) in EU Public Law, p. 36.

[101] V. Eubank, Automating Inequality, St. Martin's Press, 2019.

Applying anti-discrimination legislation within this context requires significant legal creativity and, at times, legal *acrobatics*, because these systems operate fundamentally on the principle of discrimination - that is, categorization based on distinctions such as age, gender, skin color, or place of residence. The aforementioned Amnesty International report highlights that the risk assessment system used for fraud detection in social welfare programs is both directly and indirectly discriminatory. It conflicts with numerous international conventions and EU instruments, perpetuating systemic discrimination by using criteria such as "born abroad" to assess the risk an individual poses to the social welfare system. This system is discriminatory by design, and no degree of corrective measures can sufficiently align its operation with the legal principles of anti-discrimination or, more broadly, human rights protection. A significant part of this problem lies in the lack of transparency in the algorithms and, ultimately, in the fact that it is not always clear on what basis a decision has been made—or whether it was influenced by one of the prohibited grounds for discrimination (such as race, gender, age, and so forth).

In the context of the Hague Court's ruling—and considering the deeply discriminatory nature of such systems, including the one implemented in Denmark—a similar conclusion can be drawn regarding the **Social Card System**. Due to its extreme lack of transparency, the system provides individuals with very limited opportunities to protect their rights. Moreover, there is a notable absence of fundamental assessments concerning the system's necessity, proportionality, and its overall impact on human rights. In a country where a significant portion of the population lives in poverty, this *digital poorhouse* imposes at least a dual restriction on individuals' ability to exercise their rights.

Based on the preceding analysis, we offer the following key recommendations to address the negative legal impacts of the Social Card system, as well as the broader challenges related to the automation of decision-making processes in public administration. Each recommendation serves as a starting point that requires further refinement, development, and precise definition to bring about meaningful change.

Recommendations concerning the Social Card Law:

1. The Law should be amended, particularly to ensure alignment with personal data protection regulations. Prior to any legislative amendment, an appropriate data protection impact assessment—and a broader human rights impact assessment—must be conducted, so that identified risks can be addressed directly in the legislation. Regulatory measures should establish robust mechanisms to safeguard individual rights, mandate transparency of the processes and systems underlying decision-making, and restrict the application of the system if the assessment reveals disproportionate risks to individuals.

2. The ongoing constitutional and legal review of the Law (which the Constitutional Court should initiate promptly, based on the submitted initiatives and proposals) must take into account that no adequate human rights impact assessment was conducted. This omission has significantly undermined individuals' ability to protect their rights.
3. Implementation of the Law has already shown that the Social Card system can, in specific cases, limit or violate the human rights of vulnerable groups. Given the identified risks, clear measures must be developed to monitor and address these risks. Responsibility for mitigating such risks lies solely with the authorities.
4. Until the Law is amended, individuals should be supported in using available mechanisms to protect their rights, including mechanisms before independent bodies such as the Commissioner for Information of Public Importance and Personal Data Protection, the Commissioner for the Protection of Equality, the Ombudsman, local ombudsman offices, and the courts. In this regard, providers of free legal aid and support should receive additional training ,regarding these mechanisms.
5. Employees in the social protection system should receive further training on the potential human rights impacts and risks to freedoms posed by automated decision-making processes, as well as on methods for minimizing these consequences.

Recommendations for strengthening the legal framework governing automated data processing and decision-making in public administration in Serbia:

1. Public administration must not deploy automated decision-making systems—whether fully or partially automated—without first conducting a test of legitimacy, proportionality, and necessity. This prohibition is especially important given the relatively low level of digital and technical literacy among public administration staff responsible for managing these systems.
2. Considering the power imbalance and widespread mistrust between public administration and citizens, human rights risk assessments must be carried out by independent experts through a participatory and multidisciplinary approach.
3. A significant shortcoming of the current fast-tracked legislative and system development process is the absence of an independent oversight body. Such a body must be established (or existing supervisory bodies strengthened) to identify potential risks posed by these systems and, ultimately, to determine whether Serbia's public administration is ethically and legally prepared to implement them. The oversight body should include experts from diverse

professional backgrounds and must be independent of the public administration.

4. As a minimum, systemic transparency must include both algorithm transparency—that is, information about its logic and the influence of algorithms on the decision-making process—and transparency regarding the data sources used.
5. To enable individuals to defend their rights, the principle of transparency and the right to an explanation must provide clear and understandable information regarding the algorithm's logic, the roles of both the algorithm and officials in the decision-making process, data sources, other participants involved in the procedure, third parties with access to the data, and the rights of both the individuals affected by the decision and any other individuals whose data are being processed.
6. Procedures for identifying and correcting errors must be simple, accessible, and clearly defined. These mechanisms should also be explicitly guaranteed either by the Social Card Law or by another regulation governing the use of algorithms in public sector decision-making.
7. Anti-discrimination legislation must be enforced in both the design and implementation of these systems, including a prohibition on basing decisions on data that, under the Law on the Prohibition of Discrimination, could constitute grounds for direct or indirect discrimination.
8. Public procurement procedures and contracts for the development and implementation of such systems must be transparent. The public should be involved in decision-making processes related to the introduction of these systems. Accordingly, human rights impact assessments should be conducted both when drafting legislation and when planning the procurement of services or systems for automated data processing in the public sector.
9. Algorithmic code should be made publicly available, subject to intellectual property protection rules. The public should also be informed about the stakeholders involved in planning and developing these systems, including public authorities, private entities, experts, and international organizations.
10. An individual—in this case, a public official—has an essential corrective and oversight role. Therefore, any automated data processing system that does not allow for a meaningful and substantive role for human intervention in the decision-making process should be legally prohibited.


INITIATIVE FOR ECONOMIC AND SOCIAL RIGHTS
A11