JURISdoctoria
REVUE DOCTORALE DE DROIT

*Les Cahiers d'*E-DÉLIB
2024

Human oversight of algorithmic decision-making in the public sector: insights from national and EU case law

Cristina FRATTONE

2025-2, pp. 25-55

Pour citer cet article :
Cristina FRATTONE, « Human oversight of algorithmic decision-making in the public sector: insights from national and EU case law », *Jurisdoctoria* 2025-2 [en ligne], *Les Cahiers d'e-Délib 2024*, pp. 25-55

Pour consulter cet article en ligne :
https://www.jurisdoctoria.net/wp-content/uploads/2025/07/eD-2025-2_FRATTONE.pdf

Human oversight of algorithmic decision-making in the public sector: insights from national and EU case law

CRISTINA FRATTONE

Postdoctoral research fellow, Roma Tre University

Over the past few years, the augmentation of decision-making activity through artificial intelligence (AI) technology has been at the forefront of computer science research. It promises enhanced speed, efficiency, and quality of the decision-making process. AI systems process and analyze large volumes of data in milliseconds. Furthermore, they detect correlations that may be untraceable by the human brain[1].

2 AI-driven decision-making has thus largely been deployed in both the private[2] and public sectors[3]. Focusing on the automation of decisions by the government, public administration research has described this trend as a move from "street-level bureaucracies"[4] to "screen-level" and "system-level bureaucracies", where pivotal assessments are increasingly delegated to machines[5].

[1] M. FINCK, "Automated Decision-Making and Administrative Law" in P. CANE and others (eds), *The Oxford Handbook of Comparative Administrative Law,* OUP, 2020, p. 656.

[2] S. ZUBOFF, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power* (Profile Books 2019).

[3] F. CHIUSI and others (eds), "Automating Society Report 2020", Algorithm Watch and Bertelsmann Stiftung, 2020, https://automatingsociety.algorithmwatch.org/wp-content/uploads/2020/12/Automating-Society-Report-2020.pdf accessed 15 October 2024 ; M. CHOROSZEWICZ and B. MÄIHÄNIEMI, "Developing a Digital Welfare State: Data Protection and the Use of Automated Decision-Making in the Public Sector across Six EU Countries", *Global Perspectives*, 2020, vol. 1, n°1, art. 12910, https://doi.org/10.1525/gp.2020.12910; V. EUBANKS, *Automating Inequality: How High-Tech Tools Profile, Police, and Punish the Poor*, St. Martin's Press, 2018.

[4] M. LIPSKY, *Street-Level Bureaucracy: Dilemmas of the Individual in Public Services*, 30th anniversary expanded ed, Russell Sage Foundation, 2010.

[5] M. BOVENS and S. ZOURIDIS, "From Street-Level to System-Level Bureaucracies: How Information and Communication Technology Is Transforming Administrative Discretion and Constitutional Control", *Public Admin Rev*, 2002, vol. 62, p. 174.

3 According to Public Sector Tech Watch, Member States of the European Union (EU) have implemented emerging technologies in public administration in at least 505 cases[6]. The number rises to 1152 including pilot projects, and 203 projects are under development[7].

4 Some areas of public administration are being automated thanks to machine learning, an AI technique based on inferential and probabilistic reasoning[8]. A computer observes some data to build a model, which is a set of rules, and uses it to solve future problems[9]. Machine learning, especially deep learning[10], has paved the way for increasingly complex and powerful AI systems like artificial neural networks[11]. Nevertheless, many public services are based on early AI technology, like expert systems, or a combination of simple and advanced software[12].

5 AI systems perform two main tasks in the public sector: classification and prediction[13]. Through classification, AI systems determine an individual's status as eligible for rights (such as welfare benefits and services) or obligations (such as tax debts). Through prediction, systems profile individuals based on specific characteristics or behavioral patterns to estimate a risk. For instance, they estimate the probability of recidivism and tax and welfare fraud.

6 Predictive algorithms are used to inform public officials, such as tax offices and regulators, who are in charge of the final decisions. This mechanism leaves room for human discretion, at least on paper[14].

7 Administrative decisions range from semi-automated (the final decision being made by a public servant based on assistance from the system) to fully automated (the final decision being made by the system). In practice, the boundaries between semi-automated and fully automated decisions are blurred because administrative decision-making is often the result of complex, multi-stage processes that combine semi- and fully automated instances[15].

8 In light of the foregoing, in this paper automated decision-making (hereinafter, ADM) is a wide-ranging concept that stands for decision-making processes that are fully or partially automated. More

---

[6] Public Sector Tech Watch, "Case Viewer & Statistics", Commission, Interoperable Europe, https://joinup.ec.europa.eu/collection/public-sector-tech-watch/cases-viewer-statistics accessed 15 October 2024.

[7] *Ibid.*

[8] S. RUSSELL and P. NORVIG, *Artificial Intelligence: A Modern Approach*, 4th ed., Pearson, 2020, p. 24.

[9] *Ivi* p. 651.

[10] *Ivi* p. 750.

[11] L. PORTINALE, "Mapping Artificial Intelligence: Perspectives from Computer Science" in M. EBERS, C. PONCIBÒ and M. ZOU (eds), *Contracting and Contract Law in the Age of Artificial Intelligence,* Hart Publishing, 2022, p. 9.

[12] S. RANCHORDÁS, "Empathy in the Digital Administrative State", *Duke LJ*, 2022, vol. 71, p. 1359.

[13] R. PEETERS, "The Agency of Algorithms: Understanding Human-Algorithm Interaction in Administrative Decision-Making", *Information Polity*, 2020, vol. 25, p. 507.

[14] *Ibid.*

[15] U. B. U. ROEHL and M. BALLE HANSEN, "Automated, Administrative Decision-Making and Good Governance: Synergies, Trade-offs, and Limits", *Public Admin Rev,* 2024, vol. 84, p. 1185.

precisely, ADM means a computational process that, fed by inputs and data received or collected from the environment, generates output in a wide variety of forms (such as text content, ratings, recommendations, and predictions) that is used to make decisions aimed at individuals[16]. ADM thus includes fully automated decisions and decisions formally attributed to humans, but originating from an automated data-processing operation, the result of which is not actively assessed by any person before being formalized as a decision[17]. Furthermore, ADM includes decision-making processes that are often referred to as "semi-automated" or "hybrid" decision-making since they involve both human and machine actors. In semi-automated and hybrid scenarios, human involvement can range from active participation in the decision to oversight and correction mechanisms. Put simply, the degree of automation of the system is not considered decisive for qualifying as ADM[18].

9 The definition of ADM systems adopted in this work is also technology neutral. Notably, automated administrative decisions based on simple rule-based analysis procedures rather than advanced AI technology still have major consequences for people's lives[19]. Moreover, most use cases of ADM systems in public administration thus far involve hard-coded AI models or even simpler technology that may not qualify as AI. Hence, a narrow definition of ADM systems would severely limit the scope of the analysis.

10 Manifold reasons lie behind the striving for the automation of administrative decision-making.

11 Purportedly, automation improves the efficiency of public administration. For instance, it is supposed to reduce operational costs. This means that, while the initial costs of procuring and implementing ADM systems might be considerable, marginal costs (the costs added by "producing" one additional decision) are low compared to manual decision-making[20]. Therefore, automation enables an increase in the scale of government operations. Moreover, computer programs operate faster than civil servants.

---

[16] The definition of ADM hereby provided is partially aligned with those elaborated by the European Law Institute (ELI): ELI, "Model Rules on Impact Assessment of Algorithmic Decision-Making Systems Used by Public Administration", ELI Report, 2022, www.europeanlawinstitute.eu/fileadmin/user_upload/p_eli/Publications/ELI_Model_Rules_on_Impact_Assessment_of_ADMSs_Used_by_Public_Administration.pdf; T. RODRIGUEZ DE LAS HERAS BALLELL, "Guiding Principles for Automated Decision-Making in the EU", ELI Innovation Paper, 2023, www.europeanlawinstitute.eu/fileadmin/user_upload/p_eli/Publications/ELI_Innovation_Paper_on_Guiding_Principles_for_ADM_in_the_EU.pdf.

[17] L. A. BYGRAVE, "Automated Profiling: Minding the Machine: Article 15 of the EC Data Protection Directive and Automated Profiling", *Computer Law and Security Report*, 2001, vol. 17, n°1, p. 17.

[18] T. ENARSSON, L. ENQVIST and M. NAARTTIJÄRVI, "Approaching the Human in the Loop – Legal Perspectives on Hybrid Human/Algorithmic Decision-Making in Three Contexts", *Info & Comm Tech Law*, 2022, vol. 31, pp. 125 s.

[19] Algorithm Watch, "Automating Society – Taking Stock of Automated Decision-Making in the EU", 2019, https://algorithmwatch.org/en/automating-society-2019/ accessed 15 October 2024.

[20] U. B. U. ROEHL and M. BALLE HANSEN, "Automated, Administrative Decision-Making and Good Governance", *op. cit.*, pp. 6 s.

12 These aspects are particularly relevant as public administration has compelling efficiency goals to meet in terms of time and resources. For instance, EU Member States have a precise duty to adopt decisions within a reasonable time to give full implementation to the right to good administration, which has constitutional standing in the Union as it is enshrined by Article 41 of the Charter of Fundamental Rights of the EU (CFREU)[21].

13 In addition to the increased efficiency of public administration, ADM systems allegedly promote impartiality, prevent corruption, and increase the transparency, consistency, and quality of administrative decisions due to the reduced involvement of public servants in the decision-making process and the consequent confinement of their discretion[22].

14 These arguments are not undisputed though. Efficiency gains are not straightforward due to the high costs of implementing emerging technologies. Moreover, as far as administrative discretion is concerned, automation has no unilateral effects[23]. Rather, human discretion of street-level administration persists in system-level bureaucracies due to several non-technological factors, including the impossibility of capturing all several frontline work and choices by computers, limited resources for managers to control time and attention, and work organization or the skills possessed by street-level agents[24]. The advantages of automating administrative decisions are thus open to debate.

15 Contrariwise, evidence of automation's downsides is solid, as demonstrated by the proliferation of judicial disputes on ADM systems. Concerns range from the perpetuation of existing forms of discrimination to the introduction of new types of unjustified discrimination, both caused by algorithmic bias and resulting in social exclusion[25]; from scarce transparency of the decision-making process to difficulties in providing meaningful explanations of individual outcomes[26]; from the

---

[21] On States' duty to decide within a reasonable time see Joined cases C-238/99 P, C-244/99 P, C-245/99 P, C-247/99 P, C-250/99 P to C-252/99 P and C-254/99 P, *Limburgse Vinyl Maatschappij NV (LVM) (C-238/99 P), DSM NV and DSM Kunststoffen BV (C-244/99 P), Montedison SpA (C-245/99 P), Elf Atochem SA (C-247/99 P), Degussa AG (C-250/99 P), Enichem SpA (C-251/99 P), Wacker-Chemie GmbH and Hoechst AG (C-252/99 P) and Imperial Chemical Industries plc (ICI) (C-254/99 P) v Commission of the European Communities* [2002] ECR 2002 I-8375.

[22] M. BOVENS and S. ZOURIDIS, "From Street-Level to System-Level Bureaucracies", *op. cit.*; I. SNELLEN, "Electronic Governance: Implications for Citizens, Politicians and Public Servants", *Int'l Rev Admin Sciences,* 2002, vol. 68, n°2, p. 183; *id*, "Street Level Bureaucracy in an Information Age" in I. SNELLEN and W. VAN DE DONK (eds), *Public Administration in an Information Age. A Handbook*, IOS Press 1998; A. ZUURMOND, "From Bureaucracy to Infocracy: Are Democratic Institutions Lagging Behind?" in I. SNELLEN and W. VAN DE DONK (eds), *Public Administration in an Information Age*, *op. cit.*

[23] P. A. BUSH and H. Z HENRIKSEN, "Digital Discretion: A Systematic Literature Review of ICT and Street-Level Discretion", *Information Polity*, 2018, vol. 23, p. 3.

[24] A. BUFFAT, "Street-Level Bureaucracy and E-Government", *Public Management Review,* 2015, vol. 17, p. 149.

[25] F. PALMIOTTO, "When Is a Decision Automated? A Taxonomy for a Fundamental Rights Analysis", *German Law Journal,* 2024, vol. 25, p. 210; V. EUBANKS, "Algorithms Designed to Fight Poverty Can Actually Make It Worse", *Scientific American*, 2018, vol. 319, n°5, p. 68.

[26] M. FINK and M. FINCK, "Reasoned A(I)dministration: Explanation Requirements in EU Law and the Automation of Public Administration", *European Law Review*, 2022, vol. 47, n°3, p. 376.

influence of private actors involved in the development and maintenance of ADM systems to cybersecurity risks[27]; from excessive trust in computers to the dehumanization of the decision-making process[28]. This brief, non-exhaustive overview of the risks of ADM makes it evident why public actors must implement measures to counteract its negative consequences effectively[29].

16 In policy and ethics, human oversight is a much-stressed safeguard against the negative consequences of ADM systems[30] and is considered the bedrock of human-centric AI[31]. Accordingly, human intervention and/or oversight in the context of ADM systems is required by EU and national law.

17 Saving a margin of maneuver for "authentic human reasoning" in the decision-making process purportedly gets the best out of both worlds, as society enjoys the benefits of automation without having to endure the undesired consequences of machines' inherent lack of human-like thinking[32]. As put by Koulu, human oversight is an "attractive, easily implementable and observable procedural safeguard"[33]. Moreover, human oversight heightens the perceived legitimacy of algorithmic decisions, especially when fundamental rights and freedoms are at stake[34].

18 Nevertheless, there is reason to believe that human oversight as a governance mechanism is insufficient at best[35]. Behavioral studies suggest that humans are incentivized to minimize their efforts

---

[27] S. RANCHORDÁS and Y. SCHUURMANS, "Outsourcing the Welfare State: The Role of Private Actors in Welfare Fraud Investigation", *EJCL*, 2020, vol.7, n°1, 2020, p. 5.

[28] K. YEUNG, "Why Worry about Decision-Making by Machine?" in K. YEUNG and M. LODGE (eds), *Algorithmic Regulation*, OUP, 2019; S. RANCHORDÁS, "Empathy in the Digital Administrative State", *op. cit.*

[29] UN AI Advisory Board, "Governing AI for Humanity", Interim Report, December 2023, www.un.org/sites/un2.un.org/files/ai_advisory_body_interim_report.pdf accessed 15 October 2024; J. WOLSWINKEL, "Artificial Intelligence and Administrative Law", Council of Europe, 2022, pp. 20 s., www.coe.int/documents/22298481/35097084/CDCJ%282022%2931E+-+FINAL+6+%281%29.pdf/787157dd-f386-3e51-5b93-9aac50da1489?t=1671009161932 accessed 15 October 2024.

[30] B. GREEN, "The Flaws of Policies Requiring Human Oversight of Government Algorithms", *CLS Rev*, 2022, vol. 45, n°105681, https://doi.org/10.1016/j.clsr.2022.105681; R. KOULU, "Proceduralizing Control and Discretion: Human Oversight in Artificial Intelligence Policy", *MJ*, 2020, vol. 27, p. 720.

[31] However, as highlighted by Enqvist, human-centrism and human oversight in AI "while being conceptually related notions, have different aims, focuses and manifestations". Human-centric AI applications aim to encode human values into the technical fabric of AI systems and thus proactively avoid harm. Human oversight measures, instead, are primarily procedural and of a more reactive nature as they entail the monitoring and addressing of risks, biases, and harms of AI systems in operation, and therefore are complementary to upholding accountability structures around AI. See L. ENQVIST, ""Human Oversight" in the EU Artificial Intelligence Act: What, When and by Whom?", *Law, Innovation and Technology*, 2023, vol. 15, pp. 508, 511 s.

[32] A. CLYDE, "Human-in-the-Loop Systems Are No Panacea for AI Accountability", *Tech Policy Press*, 1 December 2021, www.techpolicy.press/human-in-the-loop-systems-are-no-panacea-for-ai-accountability/ accessed 15 October 2024.

[33] R. KOULU, "Proceduralizing Control and Discretion", *op. cit.*, p. 720.

[34] A. WALDMAN AND K. MARTIN "Governing Algorithmic Decisions: The Role of Decision Importance and Governance on Perceived Legitimacy of Algorithmic Decisions", *Big Data & Society*, 2022, vol. 9, n°1, p. 10, https://doi.org/10.1177/20539517221100449.

[35] B. GREEN, "The Flaws of Policies Requiring Human Oversight of Government Algorithms", *op. cit.*, pp. 7–11.

of oversight and correction in the context of ADM systems[36]. Frontline users tend to rely completely on the data provided by the data owners. Therefore, errors spread across multiple administrative bodies through data-sharing[37]. Moreover, operators tend to uncritically accept the output of ADM systems. The longer the system performs consistently and reliably, the more likely a human operator is to trust it[38]. This leads to so-called automation bias[39] and perceived de-responsibilization by frontline public servants for automated decisions[40]. Therefore, human intervention as a governance mechanism demands a more in-depth analysis.

19 Against this background, the paper delves into human oversight in the context of ADM systems in the public sector. First, it provides a cross-disciplinary overview of human oversight drawing from literature on human-computer interaction mechanisms in automation. Second, it pinpoints the normative framework of the phenomenon. Third, relevant EU and national case law is analyzed to shed light on the interpretation and relevance of human oversight in judicial decisions. Specifically, the main object of the analysis is constituted by administrative automated decisions concerning individuals in the context of welfare and taxation, which is used for the assignment of welfare benefits and fraud detection. Additionally, the landmark judgment delivered by the European Court of Justice (ECJ) on 7 December 2023 in *OQ v Land Hessen* (hereinafter "*Schufa Holding*" or "the *Schufa Holding* case") is also examined since it represents the first interpretative guidance stemming from the Court of Justice of the EU on the automated processing of personal data for decision-making activity[41].

20 The analysis aims to highlight commonalities and differences in the reasoning of different courts and authorities. It demonstrates that concrete use cases of ADM in the public sector are likely to trigger a complex patchwork of data protection rules, AI safety rules as well as constitutional and administrative legal principles alike. To anticipate some conclusions, the research leads to a perhaps counterintuitive finding. Despite the frequent mention of human oversight by courts, the concept has not been the object of in-depth scrutiny yet. The concrete mechanisms to ensure human oversight are rarely assessed. It is often assumed in judgments that human oversight is not feasible when ADM systems are constituted of machine learning algorithms. Finally, the role of private designers and developers, who provide ADM systems and their maintenance, has been largely unexplored hitherto. Similarly,

---

[36] R. PEETERS, "The Agency of Algorithms", *op. cit.*

[37] A. WIDLAK and R. PEETERS, "Administrative Errors and the Burden of Correction and Consequence: How Information Technology Exacerbates the Consequences of Bureaucratic Mistakes for Citizens", *Int J Electronic Gov*, 2020, vol. 12, p. 40.

[38] A. TSAMADOS, L. FLORIDI and M. TADDEO, "Human Control of AI Systems: from Supervision to Teaming" *AI Ethics*, 2025, vol. 5, p. 1539, https://doi.org/10.1007/s43681-024-00489-4; V. A. BANKS, K. L. PLANT and N. A. STANTON, "Driver Error or Designer Error: Using the Perceptual Cycle Model to Explore the Circumstances Surrounding the Fatal Tesla Crash on 7th May 2016", *Safety Science*, 2018, vol. 108, p. 283.

[39] M. L. CUMMINGS, "Automation Bias in Intelligent Time Critical Decision Support Systems" in D. HARRIS and W-C. LI (eds), *Decision Making in Aviation*, Routledge, 2015.

[40] A. TSAMADOS, L. FLORIDI and M. TADDEO, "Human Control of AI Systems", *op. cit.*, p. 5.

[41] Case C–634/21 *OQ v. Land Hessen* [2023] EU:C:2023:957 (hereinafter, "*Schufa Holding*").

the accountability of high-level political actors who decide on the implementation of such systems is not touched upon by courts.

I. HUMAN OVERSIGHT AS A FORM OF HUMAN-COMPUTER INTERACTION

21 Human oversight helps ensure that an AI system does not undermine human autonomy or cause other adverse effects. There exist several mechanisms of human-computer interaction. The appropriate type and degree of human oversight may vary from one case to another.

22 For instance, validation by a human may be required before the output of the AI system becomes effective, or human review of the output may be ensured afterward. Moreover, human operators may monitor the AI system while in operation and intervene in real-time to halt the system if necessary[42].

23 In addition, human-computer interactions can take place during the learning process. These approaches can be grouped under the umbrella term of Human-in-the-loop machine learning (HITL-ML)[43]. At this stage, humans can annotate unlabeled data, interactively provide feedback on a more frequent basis compared to traditional machine learning or define the knowledge that they intend to transfer to the machine learning model.

24 Beyond the learning process, research on human-computer interactions aims to achieve so-called Usable and Useful AI[44]. Usable AI focuses on ensuring optimal user experience. Moreover, it includes mechanisms to make systems able to implement users' corrections once they are deployed, enabling an incremental improvement of the AI performance[45]. Useful AI goes further and tries to make AI models useful to society as a whole by considering human conditions and contexts[46].

25 Automated systems can play different roles in a decision-making activity. Accordingly, the interaction between the human and the machine in multi-stage processes can take many forms depending on the adopted scheme. As illustrated by Binns and Veale, computers perform three main tasks in ADM systems, namely: providing information to a decision-maker (supporting); determining which cases

---

[42] Commission, "White Paper on Artificial Intelligence – A European Approach to Excellence and Trust", COM(2020) 65 final, p. 21.

[43] R. (MUNRO) MONARCH, *Human-in-the-Loop Machine Learning*, Manning Publications, 2020.

[44] W. XU, "Toward Human-Centered AI: A Perspective from Human-Computer Interaction", *Interactions*, 2019, vol. 26, n°4, p. 42.

[45] E. MOSQUEIRA-REY and others, "Human-in-the-Loop Machine Learning: A State of the Art", *Artif Intell Rev*, 2023, vol. 56, pp. 3039–3041.

[46] *Ivi* p. 3041.

require a human assessment or additional automated processing (triaging); consolidating decisions from one or more human decision-makers (summarising)[47]. These roles can occur in the same system.

26 Multi-stage ADM processes raise several challenges, starting from the ambiguity around where to locate the final decision and the potential for upstream automation processes to foreclose downstream outcomes despite human input. To further elaborate, an intermediate automated assessment substantially constitutes a final decision if the subsequent human assessment is inconsistent due to technical, organizational, or behavioral factors[48].

II. THE NORMATIVE FRAMEWORK OF HUMAN OVERSIGHT IN THE PUBLIC SECTOR

27 Human oversight is proscribed by EU law and national law when ADM systems are used to make administrative decisions with significant effects on individuals.

28 As for the EU level, Regulations (EU) 2016/679 (General Data Protection Regulation, hereinafter "GDPR")[49] and (EU) 2024/1689 ("AI Act")[50] contain provisions on human-computer interactions in automated procedures. Both legislative acts apply to public entities and are thus relevant to ADM in the public sector.

29 The AI Act and the GDPR will likely overlap in concrete use cases. These two legislative acts differ in their scope. Public administration may qualify both as a (personal) data controller under the GDPR and a provider or deployer of an AI system. In that case, the GDPR and AI Act apply simultaneously[51].

---

[47] R. BINNS and M. VEALE, "Is That Your Final Decision? Multi-stage Profiling, Selective Effects, and Article 22 of the GDPR", *IDPL*, 2011, vol. 11, n°4, p. 319.

[48] A. TSAMADOS, L. FLORIDI and M. TADDEO, "Human Control of AI Systems", *op. cit.*, pp. 1537-1543; R. PEETERS, "The Agency of Algorithms", *op. cit.*; cf. S. ALON-BARKAT and M. BUSUIOC, "Human–AI Interactions in Public Sector Decision Making: 'Automation Bias' and 'Selective Adherence' to Algorithmic Advice", *JOPART*, 2023, vol. 33, n°1, p. 166: "While our findings as to a lack of automatic deference are encouraging in this context, the likelihood that decision-makers adhere to algorithmic advice (rather than resist it) *precisely* when predictions are aligned with group stereotypes and disadvantage minority groups is disconcerting, and speaks to potential blind spots in our ability to exercise meaningful oversight" (emphasis in the original text).

[49] 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) [2016] OJ L119/1.

[50] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down neutralize 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) [2024] OJ L, http://data.europa.eu/eli/reg/2024/1689/oj.

[51] For an analysis of the overlap between the GDPR and the AI Act see R. SCHWARTMANN and others, "Data Protection Aspects of the Use of Artificial Intelligence – Initial overview of the intersection between GDPR and AI Act", *CRi*, 2024, vol. 25, n°5, p. 145. For a comparison of provisions on the explanation of AI-driven decisions under the GDPR and the AI Act see P. HACKER and J.–H. PASSOTH, "Varieties of AI Explanations under the Law. From the GDPR to the AIA, and beyond" in A. HOLZINGER

30 Finally, ADM systems must comply with overarching principles of general administrative law. As far as human oversight is concerned, the principle of accountability is of the utmost relevance because human involvement in the decision-making process eases the identification of the public body and/or servant that is accountable for the outcome of the ADM process.

31 Moreover, human oversight intertwines with the principle of transparency and the duty to give reasons. Public servants can provide meaningful explanations to the individual affected by an administrative decision only if they know how the assessment was carried out by the ADM system. Similarly, public servants can perform meaningful human oversight only if they understand the functioning of the ADM system. Therefore, public servants need certain skills and experience to explain the decision and perform meaningful human oversight. It comes thus as no surprise that the requirement of human oversight is posited by national public law and case law[52].

32 In addition, the use of ADM by the government impinges upon human rights. Scholars have thus advocated in favor of an approach to the judicial review of automated decisions centered on human rights[53]. Domestic courts have hitherto mainly resorted to data protection law remedies in disputes concerning automated administrative decisions. However, the concrete meaning of such remedies[54] and their effectiveness are disputed[55]. A strand of the literature therefore advocates for a shift in perspective to prioritize the assessment of compliance of ADM systems with human rights as enshrined in international, EU, and domestic law. This notwithstanding, it has also been argued that the human rights framework may need adjustments to critically respond to the challenges posed by AI systems[56].

---

and others (eds), *xxAI – Beyond Explainable AI. International Workshop, Held in Conjunction with ICML 2020, July 18, 2020, Vienna, Austria, Revised and Extended Papers*, Springer, 2022, p. 343; M. NISEVIC, A. CUYPERS and J. DE BRUYNE, "Explainable AI: Can the AI Act and the GDPR Go out for a Date?", *2024 International Joint Conference on Neural Networks (IJCNN), Yokohama, Japan, 2024*, IEEE, 2024, https://doi.org/10.1109/IJCNN60899.2024.10649994 accessed 21 October 2024.

[52] G. MALGIERI, "Automated Decision-making in the EU Member States: The Right to Explanation and Other 'Suitable Safeguards' in the National Legislations", *CLS Rev*, 2019, vol. 35, n°105327, p. 22, https://doi.org/10.1016/j.clsr.2019.05.002.

[53] N. APPELMAN, R. Ó FATHAIGH and J. VAN HOBOKEN, "Social Welfare, Risk Profiling and Fundamental Rights: The Case of SyRI in the Netherlands", *JIPITEC*, 2021, vol. 12, n°4, pp. 270 s.

[54] S. WACHTER, B. MITTELSTADT and L. FLORIDI, "Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation", *IDPL*, 2017, vol. 7, p. 76; A. D. SELBST and J. POWLES, "Meaningful Information and the Right to Explanation", *IDPL*, 2017, vol. 7, p. 233; G. MALGIERI and G. COMANDÉ, "Why a Right to Legibility of Automated Decision-Making Exists in the General Data Protection Regulation" *IDPL*, 2017, vol. 7, p. 243.

[55] L. EDWARDS and M. VEALE, "Slave to the Algorithm? Why a "Right to an Explanation" Is Probably Not the Remedy You Are Looking for", *Duke L & Tech Rev*, 2017, vol. 16, p. 18.

[56] S. A. TEO, "How Artificial Intelligence Systems Challenge the Conceptual Foundations of the Human Rights Legal Framework", *Nordic Journal of Human Rights*, 2022, vol. 40, p. 216; J. NIKLAS, "Human Rights-Based Approach to AI and Algorithms" in W. BARFIELD (ed), *The Cambridge Handbook of the Law of Algorithms*, CUP, 2020, p. 541; L. MCGREGOR, D. MURRAY and V. NG, "International Human Rights Law as a Framework for Algorithmic Accountability", *Int Comp Law*, 2019, vol. 68, pp. 342 s.

33 The remainder of this section zooms in on provisions of the AI Act and the GDPR on human intervention and oversight to clarify their scope and meaning. Although such provisions aim to promote the accountability of developers and operators of ADM systems, they may not be effective as they provide vague definitions of human-computer interaction. Therefore, the concrete meaning and relevance of human intervention and oversight ultimately depend on how such loose concepts are interpreted and operationalized by domestic courts and operators.

A. The obligation to guarantee human oversight under Article 14 of the AI Act

34 Interestingly, the AI Act has two souls as it concerns data protection (akin to the GDPR) but is also an internal market instrument since its legal basis is provided by Articles 16 and 114 of the Treaty on the Functioning of the European Union[57]. This dual nature of the AI Act affects how the requirement of human oversight is conceptualized and its concrete relevance for individuals affected by automated decisions.

35 According to Article 14 of the AI Act, high-risk AI systems must be designed and developed in such a way that they can be effectively overseen by natural persons during their use. A thorough analysis of the definition of high-risk AI systems under the AI Act falls outside the scope of this paper[58]. To provide a few examples, high-risk AI systems include, among others, those used for determining accessibility and use of basic private and public services and benefits; law enforcement; migration, asylum, and border control; administration of justice and democratic processes.

36 In a nutshell, human oversight of high-risk AI systems includes several tasks, from detecting and addressing anomalies to halting the system, from correctly interpreting its output to deciding not to use it in any particular situation[59]. For this, deployers of AI systems shall adopt technical and organizational measures to ensure that such systems are operated and overseen by persons with adequate AI literacy, training, and authority[60].

B. The right to obtain human intervention under Article 22 of the GDPR

37 Under EU data protection law, decisions that impact individuals' rights and obligations—or have similarly significant effects—and are based on the processing of personal data should not be fully automated. This general prohibition is dictated by Article 22 of the GDPR, which is the bedrock of data subjects' protection against the negative consequences of ADM systems. Specifically, the first

[57] Consolidated version of the Treaty on the Functioning of the European Union [2012] OJ C326/47.

[58] The criteria for identifying high-risk AI systems are dictated by Article 6 of the AI Act and Annexes I and III to the regulation.

[59] AI Act, art 14(4).

[60] AI Act, rec 91.

paragraph of Article 22 enshrines the right not to be subject to fully automated processing, including profiling[61].

38 Importantly, ineffective human oversight should not be regarded as an adequate medium to bypass the prohibition[62]. Under Article 22 of the GDPR, ADM involves taking a particular resolution regarding a person, formal enough to be "distinguished from other steps that prepare, support, complement or head off decision-making"[63]. If the ADM merely provides input for a decision to be ultimately taken by a human who reviews and takes account of other factors, then that ADM is not "based solely" on automated processing and thus falls outside the scope of Article 22[64]. However, controllers cannot avoid the application of Article 22 by having a human merely "rubber-stamp" machine-based decisions, without actual authority or competence to alter their outcome[65].

39 Nonetheless, fully automated decisions are exceptionally allowed in a restricted number of hypotheses, namely: a) in the context of contract formation or performance, if necessary; b) when it is authorized by Union or Member State law; c) when the data subject has explicitly consented to it[66]. Moreover, where the processing relates to the special categories of personal data listed in Article 9(1) of the GDPR, full automation is allowed solely if the data subject has given express consent or where it is necessary for reasons of substantial public interest[67].

40 Even in the above-listed cases in which fully automated decisions are allowed, data subjects have nonetheless the right to obtain human intervention[68]. Article 22(3) of the GDPR provides a non-exhaustive list of safeguard measures that must be put in place by the data controller in case of fully automated processing of personal data, including the right to obtain human intervention. The latter represents a remarkable novelty of the GDPR if compared to its predecessor, namely Directive 95/46/EC (Data Protection Directive)[69]. The only safeguard against ADM mentioned in Article 15(2) of the Data Protection Directive was the opportunity to express one's views. Article 22(3) of the GDPR names the opportunity to contest the decision and the right to obtain human intervention as

---

[61] *Schufa Holding*, para 52. See also Case C–634/21 *OQ v Land Hessen* [2023] EU:C:2023:220, Opinion of AG Pikamäe, para 31; Article 29 Working Party, "Guidelines on Automated Individual Decision-making and Profiling for the Purposes of Regulation 2016/679" WP251rev.01 (6 February 2018), 19.

[62] Article 29 Working Party, "Guidelines on Automated Individual Decision-Making and Profiling", *op. cit.*, pp. 20 s.

[63] L. A. BYGRAVE, *The EU General Data Protection Regulation (GDPR) – A Commentary,* 1st ed, OUP, 2020, pp. 530–532. See also M. VEALE and L. EDWARDS, "Clarity, Surprises and Further Questions in the Article 29 Working Party Draft Guidance on Automated Decision-Making and Profiling", *CLS Rev*, 2018, vol. 34, p. 398.

[64] Article 29 Working Party, "Guidelines on Automated Individual Decision-Making and Profiling", *op. cit.*, pp. 20 s.

[65] R. BINNS and M. VEALE, "Is That Your Final Decision?", *op. cit.*, pp. 322, 324.

[66] GDPR, art 22(2).

[67] GDPR, art 22(4).

[68] GDPR, art 23(3), rec 71.

[69] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data [1995] OJ L281/31.

additional suitable safeguards[70]. In particular, human intervention should be based on an assessment of all the relevant data, including any additional information provided by the data subject, and it should be carried out by someone with the appropriate authority and capability to change the decision[71].

41 Nevertheless, the third paragraph of Article 22 of the GDPR must be read in conjunction with the second paragraph of the same article. Under Article 22(2)(b), the abovementioned safeguards, laid down by the third paragraph, do not apply when ADM has a legal basis under Union or Member State law. In such cases, suitable safeguard measures must be laid down by the relevant Union or national law[72]. In light of Recital 71 of the GDPR, such measures must include at least the right for the data subject to obtain human intervention on the part of the controller, to express his or her point of view, and to challenge the decision taken in his or her regard[73].

42 Notably, the usage of fully automated processing by public administration falls precisely within the scope of Article 22(2)(b) of the GDPR. Therefore, safeguards listed in the third paragraph, including the right to obtain human intervention, are not applicable. Admittedly, certain uses of ADM by public administration may constitute an exception, particularly in the context of public procurement, where ADM is used for contract formation or performance and therefore may fall within the scope of letter a) rather than b).

43 It follows from the above that Article 22 of the GDPR does not enshrine the right to obtain human intervention in fully automated decision-making authorized by national law in the context of social welfare and taxes. However, such a right is established by several member States' laws, such as Belgian, Dutch, German, Irish, and Hungarian law[74]. For instance, the Irish Data Protection Act 2018 specifies that fully automated decisions are allowed when they have a positive outcome for the individual concerned or when the right to request human intervention is granted[75]. Accordingly, the Irish Department of Social Protection makes use of ADM systems to assess the eligibility of individuals for social benefits, but a negative decision cannot be made without human intervention. This means that

---

[70] S. WACHTER, B. MITTELSTADT and L. FLORIDI, "Why a Right to Explanation of Automated Decision-Making Does Not Exist", *op. cit.*, p. 81.

[71] Article 29 Working Party, "Guidelines on Automated Individual Decision-Making and Profiling", *op. cit.*, p. 27.

[72] GDPR, art 22(2)(b); S. WACHTER, B. MITTELSTADT and L. FLORIDI, "Why a Right to Explanation of Automated Decision-Making Does Not Exist", *op. cit.*, p. 93.

[73] *Schufa Holding*, para 66.

[74] G. MALGIERI, "Automated Decision-making in the EU Member States", *op. cit.*, p. 22; see also S. BARROS VALE and G. ZANFIR-FORTUNA, "Automated Decision-Making Under the GDPR: Practical Cases from Courts and Data Protection Authorities", Future of Privacy Forum, 2022, pp. 10 s.

[75] Data Protection Act 2018, sec 57(1).

when a computer system indicates that a person may not qualify for a payment, the system will refer the application to a public officer[76].

44 In a nutshell, although the GDPR requires that humans are involved in ADM when decisions are based on the processing of personal data and have a significant impact on individuals, public administration can nonetheless resort to fully automated decisions if the latter ones are allowed by the applicable national law. In such cases, the existence of a right to obtain human intervention also depends on the relevant national law.

45 Therefore, human intervention under Article 22 of the GDPR plays a twofold role. On the one hand, meaningful human involvement in the decision-making process excludes the application of the safeguards listed in the third paragraph because the processing is not fully automated in that case. On the other hand, fully automated processing triggers the application of the third paragraph which mandates that some form of human involvement is nonetheless granted, as it enshrines the right of the data subject to obtain human intervention. Akin to the GDPR, several Member States' laws that provide the legal basis for fully automated processing provide for the right to obtain human intervention, thus covering those cases that do not fall under the scope of the third paragraph according to Article 22(2)(b).

46 Interestingly, the United Kingdom (UK) has taken a different approach. According to the UK Data Protection Act 2018, any kind of ADM, including fully automated processing of personal data, is allowed. However, the data subject may request the controller to reconsider the decision or make a new decision that is not based solely on automated processing[77].

47 The issue of the nature of the right to obtain human intervention—whether it is an obligation to ensure human-computer interaction or a right for individuals to exercise in order to be effective—is open to debate. If Article 22(3) of the GDPR provides for an obligation, then controllers must by default ensure some form of human control before the final decision is made. Whereas if it provides for a right that needs to be exercised, then controllers can engage in ADM without human review regarding an individual until that individual specifically requests it.

48 The latter option seems more coherent than the former one with a literal interpretation of the third paragraph since human oversight should exclude that the processing is of a fully automated nature even if it occurs at the final stage of the decision-making process in the form of validation of the ADM system's output. Indeed, any form of (meaningful) human validation of the output that is provided regardless of whether it was specifically requested by the data subject excludes that the decision is fully automated, and thus the third paragraph of Article 22 does not apply.

---

[76] Department of Employment Affairs and Social Protection, "Privacy Statement", 29 November 2019, last updated 26 August 2024, para 7.2, https://www.gov.ie/en/department-of-social-protection/organisation-information/department-of-social-protections-privacy-statement/ accessed 18 October 2024.

[77] Data Protection Act 2018, sec 14(4).

49 Furthermore, what concretely human intervention entails is not specified. As made evident by the UK Data Protection Act, the right to obtain human intervention can be interpreted as a right to ask the controller to have the decision reconsidered by a human *ex post* as well as a right to obtain a new decision following a procedure that is not based solely on automated processing. Other mechanisms of human intervention are also possible, such as the selective applications of manual processing envisaged by Irish data protection law, where human intervention is only required in those cases that could result in a negative outcome for the data subject[78].

III. CASE-LAW ON ADM IN THE PUBLIC SECTOR

A. Italy

50 Italian law contemplates ADM systems in the public sector, although it has not provided a general legal framework so far.

51 Article 3-*bis* of Law n. 241/1990 (that is the general law of administrative procedure)[79]—as modified by Law Decree n. 76/2020 (the so-called "Simplification Decree")—states: "In order to achieve greater efficiency in their activities, public administrations shall deploy computerized and telematic tools in their internal relations, between the different administrations, and between these and private parties". Automation is therefore encouraged for the sake of the principle of efficiency, which has constitutional standing under Article 97 of the Italian Constitution.

52 Interestingly, special legislation explicitly permits the use of ADM systems in two cases. Article 35(3)(a) of the Legislative Decree n. 165/2001 on public employment[80] allows the use of automation tools in public recruitment procedures. Moreover, Article 30 of the Legislative Decree n. 36/2023 (Code of Public Procurement)[81] recommends the implementation of automated solutions to make selection procedures more efficient, including AI and distributed ledger technology. Specifically, Article 19 of the Code of Public Procurement demands that public administration implement ADM systems for the evaluation of offers if it is possible.

53 The Judicial Division of the Italian Council of State (*Consiglio di Stato*) delivered several judgments on ADM systems. These rulings pinpoint the requirements for ensuring that such systems comply with administrative law principles and data protection law.

---

[78] G. MALGIERI, "Automated Decision-making in the EU Member States", *op. cit.*, p. 20 s.

[79] Law 7 August 1990 n. 241 enacting new rules on administrative procedure and the right to access administrative documents, GU 18 August 1990 n°192, 7.

[80] Legislative decree 30 March 2001 n. 165, GU 9 May 2001 n. 106, Ordinary Supplement n°112.

[81] Legislative decree 31 March 2023 n. 36, GU 31 March 2023 n. 77, Ordinary Supplement n°12.

54 The first landmark case on ADM systems dates back to April 2019 and concerned an algorithm that was used by the Italian Government to assign posts to public school teachers[82]. The applicants claimed that the assignments were illogical since the algorithm blatantly ignored teachers' scores in the examination process as well as their preferences. At the same time, assignments did not seem to have followed any other rational criteria. Specifically, the algorithm ignored the preferences expressed by teachers regardless of their score, whereas teachers with a high score were likely to have the right to assignments aligned with their preferences. Furthermore, assigned posts were distant from current posts and residences.

55 The automated decision did not include motivation. Moreover, no public officer was appointed to verify the output of the ADM system. The Council of State found that the assignments violated basic principles of administrative law, specifically impartiality, publicity, and transparency[83]. Whereas it stated that the Government can – even should – resort to ADM, it dictated two essential conditions. Firstly, the logic underpinning the decision must be transparent, including the criteria used for the decision and their respective weights[84]. Arguably, this finding relates to the model's explainability (that is the ability to show the rationale behind each step in the decision and is closely linked to justification)[85] and interpretability (that is the translation of its working principles and outcomes in human-understandable language)[86]. Secondly, the decision must be subject to judicial review[87]. Therefore, transparency serves a twofold purpose: on the one hand, it ensures that citizens understand the reasons for decisions that concern them, and, on the other hand, it enables courts to verify whether the decision was thoroughly motivated and rational[88]. Such principles were then restated and further specified by the Council of State on many occasions[89].

56 In its first judgment on ADM, the Council of State did not discuss human oversight, as it only required *ex post* human verification in the form of judicial review. However, already in December 2019, the Council included human intervention in the list of requirements. Since ADM in the public sector constitutes a decision concerning a person based on automated processing of personal data that "produces legal effects concerning him or her or similarly significantly affects him or her", the person

---

[82] Council of State, judgment 8 April 2019 n°2270.

[83] *Ivi* para 9.

[84] *Ivi* para 8.3.

[85] O. BIRAN and C. COTTON, "Explanation and Justification in Machine Learning: A Survey" in *Proceedings of the Twenty-Sixth International Joint Conference on Artificial Intelligence, Melbourne, Australia 19-25 August 2017*, IJCAI, 2017, p. 1461, https://www.ijcai.org/proceedings/2017/0202.pdf.

[86] M. GRAZIANI and others, "A Global Taxonomy of Interpretable AI: Unifying the Terminology for the Technical and Social Sciences", *Artif Intell Rev*, 2023, vol. 56, p. 3480.

[87] Council of State, judgment 8 April 2019 n°2270 para 8.2.

[88] *Ivi* para 8.4.

[89] Council of State, judgments 13 December 2019 n°8472, 8473, 8474; judgment 4 February 2020 n. 881; judgment 9 February 2021, n°1206.

(that is the data subject) has the right to obtain human intervention under Article 22 of the GDPR. "In the decision-making process, there shall be a human who is in the position to control, validate, or reverse the automated decision. In mathematics and computer science, such a model, where the machine must interact with a human being to produce the result, is named HITL (human in the loop)"[90].

57 This finding is now solid in case-law. Nevertheless, the fact that the Council of State resorted to data protection law instead of the principle of accountability in administrative law to establish the right to human intervention provides food for thought.

58 In conclusion, ADM in the public sector is encouraged in the Italian legal system but must meet three essential requirements. First, the model must be transparent and interpretable. Second, judicial review of automated decisions must be granted. Third, the individual concerned must be granted the right to obtain the intervention of a human operator who is in the position to control, validate, or reverse the decision.

B. Netherlands

59 The Dutch Government has progressively switched to digital administration[91]. On 31st August 2018, the Dutch Council of State (*Raad van State*) released an opinion on good administration and the digitalization of government, where it underlined the need to keep providing meaningful interaction with citizens and limit the expansion of automated services and decision-making[92].

60 The aforementioned risks of administrative ADM[93] tragically materialized in the Dutch child benefit scandal, which drew attention to ADM in the public sector due to its tragic consequences and ultimately led to the resignation of the Dutch Government on 15 January 2021.

61 Childcare allowance is one of the main income-dependent social supports provided to citizens of the Netherlands. When someone is entitled to a certain allowance, the amount is based on his or her financial situation at that specific time. This means that a provisional amount is paid out during the year, but the final and exact amount can only be calculated at the end of the tax year based on their total income during that year. People whose income has changed during the year may need to repay part of the allowance received. This retrospective calculation makes the system susceptible to fraud.

62 To fight social welfare fraud, the Government took a disproportionately harsh approach towards hundreds of families who applied for childcare allowance. They were wrongly accused of fraud for welfare payments received between 2013 and 2019. Their allowance was unrightfully stopped and

---

[90] Council of State, judgment 13 December 2019 n°8472, para 15.2 (translation by the author).

[91] S. RANCHORDÁS, "Empathy in the Digital Administrative State", *op. cit.*, p. 1386.

[92] *Ivi* p. 1387; Council of State, "Ongevraagd advies over de effecten van de digitalisering voor de rechtsstatelijke verhoudingen" W04.18.0230/I, 31 August 2018, paras 1, 3.1, www.raadvanstate.nl/@112661/w04-18-0230 accessed 15 October 2024.

[93] *Supra* in the introduction.

reclaimed by the Tax Administration. As a consequence, families were pushed into poverty because of exorbitant debts to the Tax Administration and therefore faced serious economic and social problems and emotional distress. More than a thousand children were taken into foster care[94]. Moreover, the Government was accused of institutionalized discrimination since sanctioned parents were often those with lower incomes or with dual nationality. Remarkably, on 17 December 2020, the parliamentary commission of inquiry (*Parlementaire ondervragingscommissie Kinderopvangtoeslag*) that was formed to investigate the matter released a report entitled "Unprecedented Injustice" (*Ongekend onrecht*)[95].

63 On 25 November 2021, the Dutch Data Protection Authority (*Autoriteit Persoonsgegevens*, hereinafter, "the Dutch DPA") fined the Tax Administration €2.75 million for data processing violations under the GDPR in relation to the allocation of childcare allowance[96]. The reason was that the ADM system used for fraud detection took into account the dual nationality of applicants as a parameter, which constituted 'unlawful, discriminatory and therefore improper' data processing, also resulting in a violation of the right to non-discrimination. The DPA found that Dutch nationality was sufficient to be processed, considering that it was the one triggering the potential benefits. Significantly, the DPA did not make any findings with regard to Article 22 of the GDPR in this case[97].

64 On 12 April 2022, the Tax Administration incurred another fine (€3.7 million) from the Dutch DPA in relation to the same matter[98]. The DPA found that the ADM system used by the Government violated several provisions of the GDPR, including not having a legal basis for processing.

65 Such events sparked lively discussion at the EU level too. The childcare allowances scandal was the object of a question addressed by the European Parliament to the European Commission. Following the opening of a parliamentary investigation[99] and the recommendations made by the Venice Commission[100], the Dutch Government announced several measures regarding the executive,

---

[94] M. HEIKKILÄ, "Dutch Scandal Serves as a Warning for Europe over Risks of Using Algorithms", *Politico*, 29 March 2022, www.politico.eu/article/dutch-scandal-serves-as-a-warning-for-europe-over-risks-of-using-algorithms/?tpcc=nleyeonai accessed 15 October 2024.

[95] Parlementaire ondervragingscommissie Kinderopvangtoeslag, "Ongekend onrecht", 15 December 2020, https://www.tweedekamer.nl/sites/default/files/atoms/files/20201217_eindverslag_parlementaire_ondervragingscommissie_kinderopvangtoeslag.pdf accessed 18 October 2024.

[96] Dutch Data Protection Authority, Decision 25 November 2021, https://autoriteitpersoonsgegevens.nl/uploads/imported/boetebesluit_belastingdienst.pdf accessed 18 October 2024.

[97] S. BARROS VALE and G. ZANFIR-FORTUNA, "Automated Decision-Making Under the GDPR", *op. cit.*, p. 36.

[98] Dutch Data Protection Authority, Decision 25 November 2021, https://autoriteitpersoonsgegevens.nl/uploads/imported/besluit_boete_belastingdienst_fsv.pdf accessed 18 October 2024.

[99] www.europarl.europa.eu/doceo/document/O-9-2022-000028_EN.html#def1 accessed 18 October 2024.

[100] Venice Commission advisory opinion (W13.22.0014/III). The Venice Commission found that "In general, the Netherlands is a well-functioning state with strong democratic institutions and safeguards for the rule of law", and that "While the shortcomings in individual rights protection uncovered in the Childcare Allowance Case are indeed serious and systemic and involve all branches of government, it appears that eventually the rule of law mechanisms in the Netherlands did work".

legislative, and judicial branches[101]. For instance, it is preparing an amendment to the national general administrative law to strengthen the rights of individuals.[102] Moreover, the EU institutions requested continuous updates on compensation measures from the Dutch Government for the annual Rule of Law reports.

66 The intensive implementation of ADM systems by the Dutch Government also led to judicial disputes, which primarily dealt with issues of transparency and justification of decisions and incidentally touched upon human oversight.

67 The leading Dutch case on administrative ADM is the decision of the District Court of The Hague (*Rechtbank Den Haag*) in *NCJM et al. and FNV v The Dutch State* (hereinafter, "the *SyRI* case")[103]. Notably, the *SyRI* case was not brought against a court of administrative law. It did not concern any administrative decisions on individuals. Rather, it was a private law claim about the compatibility of Dutch laws on the automation of social welfare fraud assessments with international and EU law, specifically the fundamental rights to privacy and data protection.

68 In this respect, the *SyRI* case is very different from the previous so-called *AERIUS* case, which was an administrative law case on an ADM system used to deliver land use permits based on nitrogen deposition[104]. In the *AERIUS* judgment of 17 May 2017, the Administrative Division of the Dutch Council of State (*Afdeling bestuursrechtspraak van de Raad van State*) stated that governmental agencies that resort to ADM systems shall be able to explain the functioning of the algorithm[105]. Hence, the fundamental choices driving the ADM process must be knowledgeable. As the *SyRI* judgment undertook a human-rights-oriented approach rather than one focused solely on the principle of transparency under general administrative law instead, it may have more far-reaching consequences than the *AERIUS* case[106].

---

[101] Letter of the Minister of the Interior and the Minister for Legal Protection to Parliament (2022), Government reaction to the Venice Commission Opinion: "The Netherlands – Opinion on the Legal Protection of Citizens".

[102] Commission, "2021 Rule of Law Report – Country Chapter on the rule of law situation in the Netherlands", SWD(2021) 721 final, pp. 12-15; *id.*, "2022 Rule of Law Report – Country Chapter on the rule of law situation in the Netherlands", SWD(2022) 519 final, pp. 16-18; *id.*, "2023 Rule of Law Report – Country Chapter on the rule of law situation in the Netherlands", SWD(2023) 819 final, pp. 20-22; all available at https://www.europarl.europa.eu.

[103] District Court of The Hague, C-09-550982-HA ZA 18-388, NL:RBDHA:2020:865, 6 March 2020 (official English translation), https://uitspraken.rechtspraak.nl/details?id=ECLI:NL:RBDHA:2020:1878&showbutton=true&keyword=njcm%2Bv%2Bthe%2Bnetherlands&idx=1 accessed 21 October 2024 ("*SyRI* case").

[104] ABRvS 17 May 2017 ECLI:NL:RVS: 2017:1259.

[105] L. CLUZEL-MÉTAYER, "The Judicial Review of the Automated Administrative Act", *Erdal*, 2020, vol. 1, pp. 101 s.

[106] A. MEUWESE, "Regulating Algorithmic Decision-making One Case at the Time: A Note on the Dutch 'SyRI' Judgment", *Erdal*, 2020, vol. 1, p. 209.

69 The *Systeem Risicoindicatie* (hereinafter "SyRI") is a risk calculation model deployed by the Dutch Government to predict social welfare fraud. SyRI has a legal basis in domestic law, specifically Section 65 SUWI Act[107] read in conjunction with Section 64 SUWI Act and Chapter 5a SUWI Decree[108].

70 SyRI produces risk reports of individuals that measure their likelihood of engaging in taxes and social security fraud, and violations of labor laws. Particularly, it was only used to analyze people in specific neighborhoods that were labeled as "problem districts" (that is, with lower socio-economic inhabitants)[109].

71 SyRI's reports are based on the processing of an enormous range of personal and sensitive data collected by different Government agencies, including data on health, finance, education, fiscal payments, and employment. For instance, SyRI has access to employment records, benefits information, personal debt reports, education, and housing history amongst others.

72 When an individual is flagged by SyRI, the case is then analyzed by the Ministry of Social Affairs and Employment before a definite risk report is filed to the relevant Government agency, which can open an investigation concerning possible fraud. The assessment thus is constituted of two phases: in the first phase the Benefits Intelligence Agency Foundation uses SyRI to flag individuals and companies with an alleged risk of fraud; in the second phase these data are assessed on their worthiness of investigation by the Ministry[110].

73 Seized by several civil society interest groups, the District Court of The Hague ruled that the Dutch legislation on SyRI was contrary to Article 8(2) of the European Convention on Human Rights (ECHR) on the right to respect private and family life. The Netherlands Trade Union Confederation (FNV) joined as a party in the claimants' proceedings.

74 Like the Italian Council of State, the District Court stated that the digitalization of public administration must, in general, be encouraged. Particularly, new technologies facilitate the exchange of data among public authorities in the context of their statutory duty to prevent and combat fraud. Combating fraud is key to avoiding the loss of public funds that are meant to finance the social security system, which is "one of the pillars" of Dutch society[111]. Against this backdrop, "the SyRI legislation is in the interest of economic wellbeing and thereby serves a legitimate purpose as adequate

---

[107] Act of 9 October 2013 to amend the Work and Income (Implementation Organisation Structure) Act and any other acts pertaining to tackling fraud by exchanging data and the effective use of data known within the government, Bulletin of Acts and Decrees 2013, 405.

[108] Decree of 1 September 2014 to amend the SUWI Decree in connection with rules for tackling fraud by exchanging data and the effective use of data known within the government with the use of SyRI, Bulletin of Acts and Decrees 2014, 320.

[109] *SyRI* case, para 6.93; see also paras 3.9 s., 4.24.

[110] *Ivi* paras 4.29 s.

[111] *Ivi* para 6.3.

verification as regards the accuracy and completeness of data based on which citizens are awarded entitlements is vitally important"[112].

75 Nonetheless, it found that the SyRI legislation violated international human rights law. The District Court considered both EU data protection law and international law and chose the latter as the most appropriate normative framework for the case at stake. More precisely, it found that Dutch domestic law violated Article 8 of the ECHR.

76 Interestingly, the claimants submitted that the program conducted fully automated processing of personal data in violation of Article 22 of the GDPR because there was no meaningful human intervention before the submission of a risk report. They argued that the mere removal of false positives could not qualify as meaningful human intervention in the meaning of the GDPR, nor could the assessment of the participating parties after receipt of a risk report[113].

77 Although the District Court scrutinized SyRI's compliance with the ECHR, not the GDPR, it nonetheless found that human oversight was insufficient. The strategy of focusing on "problem districts" introduced a significant risk of algorithmic bias, which was not neutralized by any adequate safeguard. First, no insight into the risk indicators and model was provided. Second, the fact that the reports were filed only after the Social Affairs and Employment Inspectorate verified the automated assessments produced by SyRI, including a human check for false positives and false negatives, was deemed "insufficient" by the Court[114].

78 On closer inspection, the *SyRI* judgment bears limited relevance for the governance of human oversight, though. Arguably, it does not seem that the phase of human verification was scrutinized and considered an inadequate level of human intervention, as maintained by the claimant. Rather, what the District Court found decisive in the light of Article 8 of the ECHR was the absence of transparency and explanations of the decisions, which were particularly compelling given the risk of discrimination introduced by the focus on selected districts populated by people with low incomes or different ethnic origins. Against this backdrop, the mere removal of false positives and false negatives by a human was considered insufficient as a countermeasure.

---

[112] *Ivi* para 6.4.

[113] *Ivi* para 6.57.

[114] *Ivi* para 6.94: "Based on the SyRI legislation, it cannot be assessed whether this risk is sufficiently neutralised due to the absence of a verifiable insight into the risk indicators and the risk model as well as the functioning of the risk model, including the analysis method applied by the Social Affairs and Employment Inspectorate. The circumstance that the process of data processing consists of two phases and that the analysis unit of the Social Affairs and Employment Inspectorate, following a link of the files by the IB [the Benefits Intelligence Agency Foundation], assesses the decrypted data on their worthiness of investigation, which includes a human check for false positives and false negatives, is deemed insufficient by the court. After all, the manner in which the definitive risk selection takes place is not public. Nor are the data subjects informed about how the definitive risk selection is effectuated or about the associated conclusion whether or not a risk report is submitted, while the SyRI legislation only provides for a general monitoring by the AP [Dutch Data Protection Authority] afterwards".

79 To further elaborate, the District Court did not state that human verification of false positives and negatives was an inadequate model of human oversight if compared to other possible mechanisms. Instead, the judgment is underpinned by a holistic approach to administrative ADM. The SyRI scheme was deemed unlawful due to defective transparency and explanations and risks of discrimination, which were not adequately compensated by human verification of false positives and negatives.

80 The District Court's line of reasoning is different from that followed by the Italian Council of State. Notably, the latter took a human-rights-based approach and did not grant any data protection remedies, different from the former. This notwithstanding, both courts assessed the lawfulness of administrative ADM systems through the lens of procedural fairness. The political decision to use ADM systems by public administration in the first place was not questioned[115].This aspect is particularly striking with regard to the *SyRI* case, in which the mechanism of surveillance of vulnerable people living in "problem districts" put in place by the Dutch Government was not considered discriminatory or illegal *per se*.

81 In a completely different case, the District Court of The Hague found that e-screening of applications for gun licenses did not constitute a fully automated decision under Article 22 of the GDPR[116].

82 Under Article 7(1)(c) of the Dutch Arms and Ammunition Act, a gun license may not be granted by the Dutch State if there is a reason to fear that the applicant cannot be entrusted with possession of a firearm. To assess applicants' psychological state, the Dutch Government required them to fill in a digital questionnaire that assessed their psychological state against ten risk factors, including impulsiveness, lack of empathy, egocentrism, suicidality, narcissistic harm, and extremism.

83 Two associations (Royal Dutch Hunters Society and the Royal Dutch Shooting Sports Association) seized the District Court and claimed that the e-screener breached the GDPR, as it lacked a proper legal basis and contravened the rules on automated data processing under Article 22 of the GDPR. In February 2020, the Court decided that the e-screener was not covered by the provision, as decisions regarding gun license attribution were not based solely on automated data processing. Hence, it was not prohibited, and it did not require specific safeguards other than those needed for the "ordinary" processing of personal data.

84 The Court's decision stresses that the weighting of the answers to the e-screener is carried out by a computer program based on validated algorithms that replace the assessment by a psychologist or psychiatrist. A negative result in the e-screener does not inevitably lead to a rejection of the gun license

---

[115] cf J. GOLDENFEIN, "Lost in the Loop – Who is the "Human" of the Human in the Loop?" in G. SULLIVAN, F. JOHNS and D. VAN DEN MEERSSCHE (eds), *Global Governance by Data*, CUP, forthcoming, draft available at https://dx.doi.org/10.2139/ssrn.4750634 accessed 18 October 2024.

[116] District Court of The Hague, C-09-585239-KG ZA 19-1221, NL:RBDHA:2020:1013, 11 February 2021 https://uitspraken.rechtspraak.nl/inziendocument?id=ECLI:NL:RBDHA:2020:1013&showbutton=true&keyword=avg accessed 21 October 2024.

application, though. The final decision is taken by the Dutch Police's chief constable, based on the opinion formed on the suitability of the person concerned, weighing all the information assessed. Such information includes the results of the e-screener, but also a background check of applicants and their allegations. The application is rejected if there are no clear contraindications that put the negative outcome of the e-screener into question[117].

85 The e-screening of gun license applications provides a clear example of semi-automated decision-making. In this case, the human assessment was considered pervasive enough to exclude the application of additional safeguards provided by data protection law in the case of fully automated decision-making. Strictly speaking, the finding that the ADM system merely supported the final decision on the gun license is undeniable. However, the fact that the ADM system replaces the assessment by a psychologist or psychiatrist means that this stage of the procedure is completely automated. Therefore, the ADM system must nonetheless comply with Article 22 of the GDPR. This finding is supported by the ECJ's *Schufa Holding* ruling[118], which is discussed in the fifth paragraph.

C. France

86 The Parcoursup platform used by the French government is an emblematic case of administrative ADM. Every year, Parcoursup processes more than 850,000 applications for access to higher education. Applications are submitted via a national platform and then examined at the local level by universities with the support of ADM systems.

87 This procedure was the object of intense litigation. The ADM system was challenged by a student association (Unef) for alleged violation of the duty of transparency of administrative ADM introduced by the Law for a Digital Republic of 2016. Following this reform, Article L300–2 of the French Code of Relations between the Public and the Administration (CRPA) now includes algorithms' source codes in the list of communicable administrative documents (provided that the disclosure thereof does not infringe any legal provisions like those on trade secrets or data protection)[119]. Transparency obligations are coupled with the individual's right to information. The addressee of an automated administrative decision can request the communication of the rules defining the processing and the main characteristics of its implementation.

88 Nevertheless, the French Law on Student Orientation and Success of 2018 (ORE Law)[120] regulating the Parcoursup scheme allows solely the communication of limited information concerning the local algorithms used by universities. Such algorithms are communicated only to applicants who request them, and once the decision is taken.

---

[117] *Ivi* para 4.26; S. BARROS VALE and G. ZANFIR-FORTUNA, "Automated Decision-Making under the GDPR", *op. cit.*, pp. 15, 30.

[118] Cited *supra* at para. 19.

[119] Code of Relations between the Public and the Administration (CRPA), art L311–5.

[120] Law 8 March 2018 n°166 on student orientation and success, JORF 9 March 2018 n°0057.

89 The student association brought an appeal against the refusal of communication of the local algorithm. The Administrative Tribunal of first instance allowed the appeal[121] but its decision was then overturned by the French Council of State (*Conseil d'État*)[122].

90 The Parcoursup scheme was finally brought before the French Constitutional Council (*Conseil constitutionnel*), which was required to assess whether the limitations to the right of communication established by the ORE Law were unconstitutional. The Constitutional Council delivered its judgment on 3 April 2020[123]. It found that the ORE Law impinged upon the constitutional right to communication of administrative documents enshrined in Article 15 of the Declaration of the Rights of Man and of the Citizen of 1789. Nonetheless, it upheld the limitations introduced by the ORE Law because they were justified by the public interest to the secrecy of the deliberations[124].

91 Moreover, the limitations were not considered disproportionate since the public was nonetheless informed beforehand of the general criteria of the evaluation, and specific information concerning individual assessments was communicated to candidates at their request after a final decision on their application was made.[125] However, it clarified that the applicant must be provided with information that is essential to the understanding of the decision, including criteria and methods of the individual assessment, pedagogical reasons underpinning the decision, the relative weighting of the general criteria, and criteria embedded into the algorithmic system[126].

92 Finally, the Council stated that the administration must publish a detailed report on the criteria of the evaluation and the use of ADM systems once the procedure is completed[127]. By contrast, communication of the exact configuration of the algorithm is not required.

93 This brief account of the Parcoursup cases makes it clear that administrative and constitutional disputes dealt primarily with the issues of transparency and explicability of administrative decision-making. However, the Constitutional Council considered the degree of automation of the procedure at stake too. It highlighted that the decision-making process was not fully automated: "la décision prise sur chaque candidature ne peut être exclusivement fondée sur un algorithme. Elle nécessite, au contraire, une appréciation des mérites des candidatures par la commission d'examen des vœux, puis par le chef d'établissement".

94 Remarkably, the fact that the procedure was not fully automated further supported the Council's findings on the consistency of the Parcoursup scheme with the right to communication of

---

[121] Administrative Tribunal of Guadeloupe, judgment 4 February 2019.

[122] French Council of State, decision 12 June 2019 n°427916, FR: CECHR:2019:427916.20190612.

[123] French Constitutional Council, decision 3 April 2020 n°2020-834 QPC.

[124] *Ivi* para 13.

[125] *Ivi* paras 15 s.

[126] *Ivi* para 16.

[127] *Ivi* para 17.

administrative documents under Article 15 of the 1789 Declaration[128]. Arguably, human oversight is tightly intertwined with the duty of transparency and the one to give reasons. Indeed, transparency is an enabler of effective human oversight and the ability to justify the decision.

95 This notwithstanding, the Council merely named the semi-automated nature of the procedure as one of the reasons supporting the argument of Parcoursup's compliance with the right to communication of administrative documents without further elaborating on this point. Hence, the judgment's analysis unveils that the Council established an interdependency relationship between transparency, information, and human oversight, although the rationale of this finding was not expressed.

96 The connection between transparency, information, and human oversight emerged even more clearly from a previous judgment delivered by the very same Constitutional Council on 12 June 2018[129]. In this judgment, the Council was seized to assess whether the proposed text of the Law n° 2018-493 implementing the GDPR was unconstitutional[130]. The Council evaluated the text of, among others, Article 21, which amended Article 10 of the Law n° 78-17 on Data Processing, Data Files, and Individual Liberties of 1978 to the effect that it allowed fully automated administrative decisions concerning individuals (provided that certain conditions were met). The Council verified that the renewed text of Article 10 was compliant with constitutional law, making two remarks that are particularly relevant to human oversight[131].

97 Firstly, the Council clarified that fully automated decisions concerning individuals are allowed insofar as the use of the ADM system follows legal rules and criteria defined in advance by the administration. Therefore, no transfer of decisional power from the administration to the algorithm occurs because the legal rules and criteria for the individual assessment are established by the former[132].

98 Secondly, the Council prohibited the use of self-learning algorithms to make fully automated administrative decisions based on the fact that such decisions were not explainable to the individuals concerned due to the features of this specific technology. Since Article 22 of the GDPR allows fully automated decisions only insofar as sufficient safeguards are provided, data controllers ought to at least master the algorithm and its evolutions and be able to explain its functioning in detail to the individuals concerned. When the ADM system is underpinned by advanced technology, namely self-learning algorithms, the administration cannot provide an adequate explanation of its functioning. As a consequence, self-learning algorithms cannot underpin fully automated decisions because they do not satisfy the aforementioned requirement[133].

---

[128] *Ivi* para 14.

[129] French Constitutional Council, decision 12 June 2018 n°2018-765 DC.

[130] Law 20 June 2018 n. 493 on the protection of personal data, JORF 21 June 2018 n°141.

[131] French Constitutional Council, decision 12 June 2018 n° 2018-765 DC, paras 65–72.

[132] *Ivi* para 69.

[133] *Ivi* para 71: "En dernier lieu, le responsable du traitement doit s'assurer de la maîtrise du traitement algorithmique et de ses évolutions afin de pouvoir expliquer, en détail et sous une forme intelligible, à la personne concernée la manière dont le

99 In a nutshell, the 2018 ruling requires that the administration ensure that humans are in control of ADM systems to make sure that an explanation can be provided to the individuals concerned. This condition is purportedly not met by self-learning techniques. Arguably, the Council's reasoning touched upon human oversight and its limits, although these issues were analyzed through the lenses of the principle of transparency and the right to an explanation. The consideration paid to human oversight is evident from the requirements that the ADM system follows preset rules established by the administration and data controllers "master" the algorithm and its evolution.

IV. INSIGHTS FROM THE ECJ'S *SCHUFA HOLDING* RULING

100 On 7 December 2023, the ECJ (First Chamber) delivered its first landmark judgment on the interpretation of Article 22 of the GDPR in the *Schufa Holding* case[134]. Specifically, the latter dealt with the use of ADM systems by private actors for credit scoring.

101 Creditworthiness assessment entails the evaluation of the ability of the consumer to pay a loan or mortgage back on time. Financial institutions must thoroughly assess the consumer's creditworthiness before a credit agreement is concluded[135]. The assessment should consider all necessary and relevant factors that influence a consumer's ability to repay the credit. Notably, it should be based on accurate information about the consumer's income and expenses and other financial and economic circumstances. Collected data should be necessary and proportionate to the credit's nature, duration, value, and risks. That information may include evidence of income or other sources of repayment, information on financial assets and liabilities, or information on other financial commitments.

102 The rationale of creditworthiness assessment is to prevent irresponsible lending practices and over-indebtedness in the consumer's best interest[136]. However, it is of the utmost importance that such an assessment is as accurate as possible since it ultimately determines a consumer's access to financial resources and essential services such as housing, electricity, and telecommunication services.

103 With automated credit scoring, human decision-making is augmented or substituted by using ADM systems to assess the creditworthiness of consumers by credit providers. Automated credit scoring

---

traitement a été mis en œuvre à son égard. Il en résulte que ne peuvent être utilisés, comme fondement exclusif d'une décision administrative individuelle, des algorithmes susceptibles de réviser eux-mêmes les règles qu'ils appliquent, sans le contrôle et la validation du responsable du traitement".

[134] Cited *supra* at para. 19.

[135] Directive (EU) 2023/2225 of the European Parliament and of the Council of 18 October 2023 on credit agreements for consumers and repealing Directive 2008/48/EC [2023] OJ L2225/1 ("Consumer Credit Directive"), art 18; Directive 2014/17/EU of the European Parliament and of the Council of 4 February 2014 on credit agreements for consumers relating to residential immovable property and amending Directives 2008/48/EC and 2013/36/EU and Regulation (EU) No 1093/2010 OJ L60/34 ("Mortgage Credit Directive"), art 18, art 20.

[136] Consumer Credit Directive, rec 54.

must comply with the GDPR and, if underpinned by AI algorithms, the AI Act. The latter classifies AI systems used for credit scoring as high-risk AI systems[137]. Therefore, Article 14 of the AI Act, requiring human oversight for high-risk systems, applies to automated credit scoring[138].

104 Under German law, the private company Schufa is allowed to perform credit scoring activity. It estimates the creditworthiness of third parties and provides such information to its contractual partners. Most notably, Schufa's partners include financial institutions that use the information provided by the company when processing consumers' applications for loans or mortgages.

105 Schufa establishes a prognosis on the probability of a future behaviour of a person ("score"), such as the repayment of a loan, based on certain characteristics of that person, on the basis of mathematical and statistical procedures. The establishment of scores ("scoring") is based on the assumption that, by assigning a person to a group of other persons with comparable characteristics who have behaved in a certain way, similar behaviour can be predicted.

106 In the *Schufa Holding* case, a consumer (OQ) was refused the granting of a loan by a third party after having been the subject of negative information established by SCHUFA and transmitted to that third party. OQ applied to Schufa to receive information on registered personal data and to request cancellation of data that was allegedly incorrect.

107 In response to that request, Schufa informed the consumer of her score and outlined, in broad terms, the methods for calculating the scores. However, referring to trade secrecy, it refused to disclose the elements taken into account for that calculation and their weighting criteria. Furthermore, Schufa argued that credit scoring did not constitute a decision within the meaning of Article 22 of the GDPR, as it merely supported the final decision by the third party.

108 The ECJ's ruling originated from the appeal brought before the District Administrative Court of Wiesbaden (Verwaltungsgericht Wiesbaden) by OQ against the negative decision by the Hessen Data Protection Authority (Hessischer Beauftragter für Datenschutz und Informationsfreiheit) on her complaint, lodged to obtain an order against Schufa, granting her access to her data.

109 In consistency with Advocate General Pikamäe's opinion, the ECJ maintained that the creditworthiness assessment conducted by Schufa met the definition of "a decision based solely on automated processing" under Article 22 of the GDPR, more specifically that of profiling under Article 4(4). This finding was based on the facts of the case as referred by the national administrative court. The latter explicitly said that Schufa provided for the automated establishment of a probability value based on personal data relating to a person and concerning that person's ability to repay a loan in the future[139].

---

[137] AI Act, art 6(2) and Annex III, point 5(b).

[138] N. VARDI, *Creditworthiness and "Responsible Credit". A Comparative Study of EU and US Law,* Brill Nijhoff, 2022, p. 97; N. AGGARWAL, "The Norms of Algorithmic Credit Scoring", *CLJ*, 2021, vol. 80, pp. 42 s.

[139] *Schufa Holding*, para 47; *Schufa Holding* [2023] EU:C:2023:220, Opinion of AG Pikamäe, para 33.

110 Most importantly, the ECJ clarified that the concept of "decision" which either produces "legal effects" concerning the data subject or "similarly significantly affects him or her" within the meaning of Article 22(1) of the GDPR is capable of including several acts which may affect the data subject in many ways. That concept is broad enough to encompass the result of calculating a person's creditworthiness in the form of a probability value concerning that person's ability to meet payment commitments in the future[140]. According to Recital 71 of the GDPR, the term 'decision' covers, for example, the automatic refusal of an online credit application[141].

111 As regards the condition that the decision must produce "legal effects" concerning the person at issue or affect him or her 'similarly significantly' for Article 22 of the GDPR to apply, the ECJ stated that the fact that the activity carried out by Schufa constituted only an intermediate stage of the assessment conducted by its partners did not exclude the application of the provision. From the factual findings of the referring court, it was apparent that the final decision of the third party to whom the probability value was transmitted drew "strongly" on that value, as the transmission of an insufficient probability value led, in almost all cases, to the refusal of that bank to grant consumers the loan applied for[142].

112 For all of the abovementioned reasons, the ECJ ruled that "in circumstances such as those at issue in the main proceedings, in which the probability value established by a credit information agency and communicated to a bank plays a determining role in the granting of credit, the establishment of that value must be qualified in itself as a decision producing vis-à-vis a data subject "legal effects concerning him or her or similarly significantly [affecting] him or her" within the meaning of Article 22(1) of the GDPR"[143].

113 The opposite solution—that a fully automated assessment heavily influencing the outcome of a semi-automated decision-making process does not constitute a decision within the meaning of Article 22 of the GDPR—would lead to a risk of circumventing said provision in circumstances in which more than two stakeholders are involved. There would thus be a lacuna in legal protection if a restrictive interpretation of that provision was retained, according to which the establishment of the probability value must only be considered as a preparatory act and only the act adopted by the third party can, where appropriate, be classified as a "decision" within the meaning of Article 22(1) of the GDPR. In that situation, the establishment of a probability value such as that at issue in the main proceedings would escape the specific requirements provided for in Article 22(2) to (4) of the GDPR, even though that procedure is based on automated processing and that it produces effects significantly affecting the data subject to the extent that the action of the third party to whom that probability value is transmitted draws strongly on it[144].

---

[140] *Schufa Holding*, para 46; *Schufa Holding*, Opinion of AG Pikamäe, para 38.

[141] *Schufa Holding*, para 45.

[142] *Ivi* para 48.

[143] *Ivi* para 50.

[144] *Ivi* paras 61 s.

114 Furthermore, where the final decision significantly affects the data subject, like those on loan applications, risks of discriminatory effects—based on racial or ethnic origin, political opinion, religion or beliefs, trade union membership, genetic or health status, or sexual orientation—are particularly compelling. Additional safeguard measures other than those already required for "ordinary" data processing are therefore needed[145].

115 If Article 22 of the GDPR only applied to the final step of the decision-making process, data controllers could place contentious automated processing of data upstream to circumvent the regulation. The stringent legal requirements imposed on automated profiling by Article 22 could thus be avoided[146].

116 Although the *Schufa Holding* ruling concerns the use of ADM systems by private actors, it has important consequences for the use of this technology by public administration. The GDPR applies to both private actors and public actors. Hence, the relevance of the ECJ's interpretation of Article 22 of the GDPR to the phenomenon at stake. When an administrative decision is made with the aid of ADM systems and the outcome of the computerized assessment has a critical impact on the final decision, that assessment qualifies as a fully automated decision within the meaning of Article 22 of the GDPR. Therefore, no meaningful human assessment occurs if the automated scoring is taken as "ground truth" by the officer in charge of the next decision-making steps.

CONCLUSIONS

117 The paper has elaborated on the interplay between different branches of law in the regulation of the use of ADM systems by public administration bodies, including fully and semi-automated processes. It has been demonstrated that ADM impinges upon citizens' fundamental rights and basic principles of administrative law, data protection law, and AI safety law.

118 The scope and efficacy of human intervention in ADM are prominent from a legal viewpoint. Nevertheless, the literature has repeatedly pointed out the intrinsic limitations of human oversight as a governance mechanism.

119 Human intervention is thus essential, although it may be substantially ineffective for several technical, organizational, and behavioral reasons. Therefore, the inclusion of summary human verification must be deemed inadequate for compliance with relevant EU and national law. Most prominently, inaccurate human oversight should not shield public administration and (private or public) providers of ADM systems from their liability for wrongdoings against citizens caused by automated administrative decisions[147].

---

[145] *Ivi* para 59.

[146] R. BINNS and M. VEALE, "Is That Your Final Decision?", *op. cit.*

[147] J. GOLDENFEIN, "Lost in the Loop", *op. cit.*, p. 16.

120 However, these inherent limitations of human oversight may not suggest abandoning such a measure altogether. Rather, they may prompt further socio-technical research into human-computer interaction mechanisms to implement more effective organizational and technical designs.

121 From a legal standpoint, what seems more problematic is the looseness of the concept of human oversight. Despite the fundamental role attributed to human oversight, legal provisions and judicial decisions have failed to define it with sufficient precision hitherto. Although human oversight is in the spotlight, its concrete meaning is largely obscure.

122 Human oversight is a wide concept that encompasses different mechanisms of surveillance over a computer's development and functioning[148]. It can thus occur at different stages of developing and deploying an AI system. Intuitively, oversight has different orientations and purposes. Therefore, it requires different competencies and expertise, depending on whether it is to be performed during the development or the functioning of a system, and at which exact phase of these two stages. As summarized by Enqvist, the concrete meaning of human oversight depends on what aspects of a system process the oversight is to be aimed at, when the oversight is to be performed, and who is to perform it[149].

123 Excessive reliance on human oversight without a clear understanding of it deprives this safeguard of any effectiveness. Rather than protecting individuals affected by automated decisions, human oversight risks benefiting high-level political actors by limiting their accountability for top-level decisions, such as deciding to deploy AI systems in the first place. Arguably, human oversight is not as influential on the final output as previous choices that are made at the stage of designing and developing the AI system[150].

124 With governmental ADM, administrative discretion is mostly exercised by those responsible for programming the decision-making process and translating the legislation into software[151]. The accountability typically associated with a public servant making a decision is streamlined throughout the AI pipeline. Hence, the administrative authority outsources some discretionary power to AI providers, mostly private actors.

125 In light of the above, those creating and implementing ADM systems should be accountable for their actions and decisions[152]. A more ethical approach to political decisions on whether and how to

---

148 See E. MOSQUEIRA-REY and others, "Human-in-the-Loop Machine Learning: A State of the Art", *op. cit.*

149 L. ENQVIST, "Human Oversight", *op. cit.*

150 V. DIGNUM, *Responsible Artificial Intelligence: How to Develop and Use AI in a Responsible Way*, Springer, 2019.

151 S. ZOURIDIS, M. VAN ECK and M. BOVENS, "Automated Discretion" in T. EVANS and P. HUPE (eds), *Discretion and the Quest for Controlled Freedom*, Palgrave Macmillan, 2020, pp. 323–327. For a thorough account of how supervised machine learning systems are developed, see P. FRIEDL, "Dis/similarities in the Design and Development of Legal and Algorithmic Normative Systems: The Case of *Perspective API*", *Law, Information and Technology*, 2023, vol. 15, pp. 27–31, 58.

152 J. GOLDENFEIN, "Algorithmic Transparency and Decision-Making Accountability: Thoughts for Buying Machine Learning Algorithms" in Office of the Victorian Information Commissioner (ed), *Closer to the Machine: Technical, Social, and Legal Aspects*

implement ADM systems is thus expected[153]. Furthermore, the implementation of ADM systems by the government must be grounded on national law, enacted following a democratic debate on the necessary balance between administrative efficiency and the protection of citizens' rights, such as the right to respect for private life, equality, and non-discrimination[154].

126 Profiling technologies are not simply "scientific" and "neutral", thus the underlying policy choices involved in their deployment must be seriously questioned[155]. National laws overlook the importance of establishing clear standards for deciding which decisions should be automated and which should not; and appropriately designed systems for transparency, review, and appeal.

127 Researchers have also pointed to the difficulties of reconciling governmental ADM with the rule of law.[156] According to the rule of law, public administration cannot act freely as it deems desirable to achieve political or efficiency goals[157]. On the contrary, it has to remain within the boundaries and respect the constraints established by the law. Dimensions of the rule of law that are challenged by ADM systems include the predictability, coherence, and justification of State's action, procedural fairness, and effectiveness of judicial review.

---

of AI, Office of the Victorian Information Commissioner, 2019, https://ovic.vic.gov.au/wp-content/uploads/2019/08/closer-to-the-machine-web.pdf accessed 18 October 2024.

[153] J. NIKLAS, "Human Rights-Based Approach to AI and Algorithm" in W. BARFIELD (ed), *The Cambridge Handbook of the Law of Algorithms*, CUP, 2020, pp. 534–542; T. CARNEY, "Robo-Debt Illegality: The Seven Veils of Failed Guarantees of the Rule of Law?", *Altern Law J*, 2019, vol. 44, p. 5; J. B. BULLOCK, "Artificial Intelligence, Discretion, and Bureaucracy", *Am Rev Pub Admin*, 2019, vol. 49, p. 751.

[154] E. DEGRAVE, "The Use of Secret Algorithms to Combat Social Fraud in Belgium", *Erdal*, 2020, vol. 1, pp. 173, 177.

[155] UN General Assembly, "Extreme Poverty and Human Rights", 11 October 2019, UN Doc A/74/493, p. 5. See also N. APPELMAN, R. Ó. FATHAIGH and J. VAN HOBOKEN, "Social Welfare, Risk Profiling and Fundamental Rights", *op. cit.*, pp. 270 s.

[156] M. ZALNIERIUTE, L. BENNETT MOSES and G. WILLIAMS, "The Rule of Law and Automation of Government Decision-making", *MLR*, 2019, vol. 82, n°3, p. 425.

[157] G. NAPOLITANO, "The Rule of Law" in P. CANE and others (eds), *The Oxford Handbook of Comparative Administrative Law,* OUP, 2020, p. 427.

RESUME :

Les administrations publiques des États européens recourent de manière croissante à des systèmes de décision automatisée. Le contrôle humain est largement reconnu comme une garantie essentielle, permettant de s'assurer que les bénéfices de l'automatisation ne compromettent ni l'équité ni la justice des décisions individuelles. Après de brèves remarques sur l'interaction entre l'humain et la machine, l'article expose le cadre normatif applicable au contrôle humain. Il mène ensuite une analyse comparative incluant les jugements des juridictions nationales sur les décisions automatisées dans des domaines tels que les prestations sociales ou la fiscalité, ainsi que l'arrêt « Schufa » de la Cour de justice relatif au credit scoring. Bien que ce dernier concerne le secteur privé, cet arrêt clarifie la portée de l'article 22 du Règlement général sur la protection des données, applicable également au secteur public. S'appuyant sur cette jurisprudence, l'article tire des conclusions quant au rôle jusqu'ici attribué au contrôle humain. Il met par ailleurs en évidence certains aspects d'ordre sociotechnique qui demeurent à ce jour insuffisamment pris en compte par les juridictions.

SUMMARY:

Public administrations in European states are increasingly relying on automated decision-making (ADM) systems. Human oversight is widely recognized as a fundamental safeguard to ensure that the benefits provided by automation do not come at the expense of fairness and justice. Following brief preliminary remarks on human-computer interaction, this article outlines the normative framework for human oversight. It then conducts a comparative analysis of relevant case law, including decisions by domestic courts on ADM systems in areas such as social benefits and taxation, as well as the ECJ's ruling in the "Schufa" case on credit scoring. Although the latter case concerns the use of ADM in the private sector, it sheds much-needed light on the scope of Article 22 of the General Data Protection Regulation, which also applies to the public sector. Drawing from this body of case law, the article assesses the role fulfilled by human oversight in ADM systems thus far. It also highlights certain socio-technical aspects of human-machine interaction that remain insufficiently addressed by the courts to date.