Maastricht University
Faculteit der Rechtsgeleerdheid

Maastricht Centre
for European Law

Scoring Systems in the General Data Protection Regulation and Artificial Intelligence Act: A Critical Appraisal

Letizia Comel

MCEL Master's Thesis Series
No 2025/03

The MCEL Master's Thesis Series seeks to give excellent students the opportunity to publish their final Master's theses and to make their work accessible to a wide audience.

Those wishing to submit papers for consideration are invited to consult our website and to send their work to mcel@maastrichtuniversity.nl.

Published in Maastricht, May 2025

Faculty of Law
Maastricht University
Postbox 616
6200 MD
Maastricht
The Netherlands

This paper is to be cited as MCEL Master's Thesis Series 2025/03

Abstract

Reliance on scoring systems, rendered even more prominent by artificial intelligence (AI), entails the assessment of individuals based on diverse datasets to generate scores that influence critical decisions in areas such as creditworthiness, social services, and employment. This trend raises profound concerns regarding fundamental rights, particularly data protection, non-discrimination, and the potential for social control, especially in relation to sensitive biometric information.

This research examines the regulatory framework governing AI-driven scoring systems in the EU, focusing on the General Data Protection Regulation (GDPR) and the AI Act (AIA). The central research question explores how these legal instruments regulate scoring systems and safeguard personal data, with a specific emphasis on biometric data and the potentially under-protected category of 'biometric-based' data.

The analysis considers the GDPR's provisions on automated decision-making, particularly Article 22, as interpreted by the Court of Justice in the SCHUFA case. Additionally, it examines the AIA's risk-based approach, which classifies credit scoring as high-risk and explicitly prohibits social scoring systems akin to those implemented in China.

Despite these regulatory safeguards, the research argues that ambiguities and gaps remain. A key critique concerns the narrow definition of 'biometric data' under the GDPR and AIA, which requires unique identification capabilities. This restriction may exclude 'biometric-based' data from enhanced protections, creating potential loopholes for systems analysing characteristics such as accents or facial expressions in credit and hiring decisions. Through doctrinal legal analysis, case law review, comparative perspectives, and hypothetical scenarios, this analysis aims to illuminate these regulatory challenges and identify potential circumventions. Ultimately, it seeks to contribute to the broader discourse on ensuring AI-driven scoring systems align with fundamental rights and European societal values.

List of Abbreviations

ADM	Automated Decision-Making
AG	Advocate General
AI	Artificial Intelligence
AIA	Artificial Intelligence Act
Art.	Article
CFREU	Charter of Fundamental Rights of the European Union
CJEU	Court of Justice of the European Union
ECJ	European Court of Justice
EU	European Union
GDPR	General Data Protection Regulation
SCS	Social Credit System
TFEU	Treaty on the Functioning of the European Union

Table of Contents

1. Introduction and Problem Statement

What if every action you have taken in life could be reduced to a single number, one that has the power to influence your future activities and interactions with both individuals and institutions? Although this concept might seem improbable, such a phenomenon, known as 'scoring', already exists to varying extents.

Scoring systems, broadly defined, entail the evaluation of individuals based on diverse datasets, culminating in numerical scores that influence various decision-making processes, which may pertain to creditworthiness, such as the approval of loans, access to social services, like housing or electricity contracts, and candidate recruitment and employability.[1] These systems convert qualitative human attributes and behaviours, from education and assets to cultural background, into quantitative data, enabling the prediction of future actions and facilitating evaluative decisions.[2]

In the rapidly evolving landscape of Artificial Intelligence (AI), the advancement of scoring practices is progressing swiftly, while their regulation remains notably ambiguous.[3] Furthermore, the application of these technologies raises substantial questions and concerns, especially regarding privacy, discrimination, and the potential for social control.[4] A critical area of focus is the fundamental right to personal data, whose protection in the EU is explicitly enshrined in Art. 16(1) of the Treaty on the Functioning of European Union (TFEU)[5] and Art. 8(1) of the Charter of Fundamental Rights of the EU (CFREU).[6]

---

[1] Lina Dencik and others, 'Data Scores as Governance: Investigating Uses of Citizen Scoring in Public Services. Project Report' [2018] Data Justice Lab Cardiff University 10.

[2] ibid.

[3] Danielle Keats Citron and Frank Pasquale, 'The Scored Society: Due Process for Automated Predictions' (2014) 89 Washington Law Review.

[4] Scott McLean and others, 'The Risks Associated with Artificial General Intelligence: A Systematic Review' (2023) 35 Journal of Experimental & Theoretical Artificial Intelligence 649.

[5] Consolidated Version of the Treaty on the Functioning of the European Union [2012] OJ C 326/47.

[6] Charter of Fundamental Rights of the European Union [2012] OJ C 326/391.

Particular attention is given to highly sensitive and intrusive information, such as biometric data, which encompass, for instance, fingerprints and iris scans.[7]

This Master's Thesis investigates the regulatory framework governing scoring systems, concentrating on the General Data Protection Regulation (GDPR)[8] and the AI Act (AIA),[9] which has recently entered into force. These two Regulations have been selected to guide the study towards an analysis that explores the interplay between the advancement of AI-based scoring practices and the safeguarding of personal data within the European Union (EU), specifically biometric ones. The examination will reveal whether and how these legislative instruments address the challenges posed by scoring systems, which are increasingly – often covertly – employed across various sectors.[10]

This essay will answer the following question: "*How do the General Data Protection Regulation and the Artificial Intelligence Act regulate scoring systems and protect personal data, specifically biometric and biometric-based ones?*".

As it will be delineated, the GDPR establishes a robust framework for safeguarding personal data and mandates specific, even if sometimes debatable, lawful grounds for its processing, particularly for sensitive data such as biometric data, as defined under Art. 4(14) GDPR. However, this essay critiques the narrowness of this definition, as it requires this information to necessarily allow for the unique identification of individuals.

The AIA, still at the beginning of its journey, complements the GDPR by specifically addressing AI systems through a risk-based approach, categorising certain practices, including credit scoring, as high-risk and placing them under

[7] Iynkaran Natgunanathan and others, 'Protection of Privacy in Biometric Data' (2016) 4 IEEE Access 880.

[8] 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, GDPR) [2016] OJ L 119/1.

[9] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act, AIA) [2024] OJ L 9/144.

[10] Citron and Pasquale (n 3).

stringent regulatory oversight. Social scoring, which involves the evaluation of individuals based on personal characteristics, is instead explicitly prohibited.

Despite these regulatory efforts, it is believed that ambiguities and gaps persist. This lack of clarity could potentially allow for the circumvention of legislative safeguards. The distinction between permissible high-risk activities and prohibited practices is crucial, yet not always straightforward, leading to legal uncertainties.

Within the EU, various initiatives employing scoring systems, and in general automated decision-making (ADM) practices, are already in place, reflecting a spectrum of intrusiveness. While no concrete examples of scoring through biometric or biometric-based data have been fully implemented or planned outside the law enforcement sector, the potential for such applications is evident. Consequently, the increasing integration of AI systems into decision-making processes necessitates a thorough examination of the legal implications, particularly concerning fundamental rights.

This essay will explore concrete examples and hypothetical scenarios to highlight potential loopholes and areas requiring further legislative attention. The following Chapters will systematically dissect the various aspects of scoring systems and their associated challenges. First, Chapter 1 will introduce the concept(s) of scoring and its application across various sectors. Chapter 2 will then delve into the GDPR and AIA, examining specific provisions and case law related to ADM - that is the recent interpretation of the Court of Justice (ECJ) in the SCHUFA case scoring processes, and the use of biometric and biometric-based data. Finally, Chapter 3 will introduce the concept of biometric categorisation, analysing its potential similarities and differences to scoring through biometric data, and will then present a comparative analysis of practices within the EU and beyond, such as the famous Social Credit System in China.

With regard to methodology, the research presents concrete examples to illustrate key concepts and facilitate comprehension, alongside a comparative analysis of various national and international regulatory systems, both within and outside the EU. Additionally, a doctrinal approach is employed to thoroughly examine the legal principles and frameworks governing scoring systems. This involves a detailed analysis of primary legal sources, including legislation, case

law, and regulatory guidelines, to understand how the legal doctrines are applied and interpreted in practice.

The literature reveals certain limitations within the existing case law of the Court of Justice of the European Union (CJEU) and scholarly work, particularly due to the novel nature of the AIA and the dynamic development of AI technologies. Although substantial discourse exists on the GDPR, the recent introduction of the AIA highlights a gap in comprehensive legal analysis.

This Master's Thesis aims to bridge this gap by contributing to the existing body of knowledge, offering insights into the complex regulatory landscape, and proposing pathways to ensure that scoring practices are deployed in ways that uphold individual rights and societal values.

2. Scoring Systems and Fundamental Rights Implications

2.1 Scoring Systems Definition(s)

The first chapter of this LLM Thesis aims to introduce the concept of scoring and its possible fields of adoption. By analysing national and EU legislation, data protection authorities' definitions, as well as case law, we will first determine how scoring systems can be described and which practices might be useful to fulfil the scope of this research.

In the realm of EU law, a definitive and universally agreed-upon definition of the term 'scoring' seems to remain conspicuously absent.[11] Rather than encountering a comprehensive explication *per se*, what emerges are delineations of distinct types or modalities of scoring, which will later be analysed. However, it is noteworthy that when examining national legal frameworks, a delineation has been elucidated, for instance, within German law. According to the provision, scoring is framed as the utilisation of a probability value on the prospective actions of an individual, employed to deliberate upon

[11] Katja Langenbucher and Patrick Corcoran, 'Responsible AI Credit Scoring – A Lesson from Upstart.Com' in Emilios Avgouleas and Heikki Marjosola (eds), *Digital Finance in Europe: Law, Regulation, and Governance* (De Gruyter 2021) <https://www.degruyter.com/document/doi/10.1515/9783110749472-006/html> accessed 21 February 2024.

the establishment, implementation, or cessation of a contractual association with said individual.[12]

More in general, without taking into consideration its different categories, scoring is usually understood as the process of categorising and segmenting the population based on diverse datasets, occasionally involving rating and ranking through a numerical value, to pinpoint particular risks and behaviours.[13] Specifically, an evaluation or assessment of the subject is made by gathering pertinent data and interpreting it using an algorithm to generate a judgment, rating, or measurement, which can lead to incentives or penalties based on compliance with underlying objectives.[14] Therefore, as the individual aligns more closely with the expectations encoded in the algorithm, their rating score increases and so do their chances of receiving rewards. As an example, we could consider its use in job applications: applicant tracking systems employ scoring algorithms to evaluate resumes based on criteria like education, experience, and skills. Higher scores prioritise candidates for further consideration, streamlining the initial screening process for both companies and applicants.[15]

From this brief overview, it is discernible what the key elements of scoring entail. This practice (i) involves the assessment of probabilities concerning individuals' and/or groups' actions, (ii) relies on pertinent data and typically yields quantitative outcomes, thereby facilitating comparative analysis, and (iii) its principal function lies in future prediction, serving as a decision-support tool by furnishing objective assessment. This technical capability, which transforms an expanding range of activities and human behaviours into quantifiable data points and formats, is intended to facilitate the investigation of such information. The primary objective of this process is to infer probabilities, anticipate human

[12] Cfr. Paragraph 31 of the Bundesdatenschutzgesetz (Federal Law on data protection) of 30 June 2017 (BGBI. I, p. 2097; 'the BDSG'), 'Protection of trade and commerce in the context of "scoring" and credit reports'.

[13] Dencik and others (n 1).

[14] Larry Catá Backer, 'Measurement, Assessment and Reward: The Challenges of Building Institutionalized Social Credit and Rating Systems in China and in the West' [2017] Conference: The Chinese Social Credit System 2017.

[15] 'Candidate Scoring' (*HiPeople*, 2023) <https://www.hipeople.io/glossary/candidate-scoring> accessed 20 July 2024.

behaviour, and make well-informed decisions based on these predictions.[16] Consequently, scoring methodologies can be regarded as essential elements of the 'datafication' paradigm, as they involve the conversion of online and offline actions into measurable data.[17]

The phenomenon of the 'scored society' is becoming progressively evident, considering these systems are being used across several sectors such as insurance, banking, employment, and numerous other domains.[18] This trend is largely facilitated by the emergence of scalable ADM systems, in which the authority is initially transferred to another individual or legal entity, whose task is to utilise automatically executed models to carry out the prescribed actions.[19] These enable swift and efficient processing of vast amounts of data, allowing quicker assessment and evaluations. However, this tendency reflects a growing reliance on quantifiable metrics to shape decisions and interactions in society that can cause several fundamental right implications and detrimental outcomes.[20] These will be analysed in the next parts.

2.2 Focus on Scoring Systems and Fundamental Rights at Stake

In the pursuit of this research, the following sub-sections aim at first undertaking a detailed analysis of two prominent areas where AI-based scoring systems hold recognition, namely credit assessment and social evaluation. Although, as illustrated above with the recruiting example, scoring practices can be applied across various domains, this research mostly focuses on the two aforementioned areas. These are indeed the fields where this methodology appears to be most widely acknowledged, both within the EU and globally.

---

[16] Lina Dencik and others, 'The "Golden View": Data-Driven Governance in the Scoring Society' (2019) 8 Internet Policy Review <https://policyreview.info/node/1413> accessed 20 July 2024.

[17] Viktor Mayer-Schönberger and Kenneth Cukier, *Big Data: A Revolution That Will Transform How We Live, Work and Think* (1. publ, Murray 2013).

[18] Citron and Pasquale (n 3).

[19] 'Automating Society Taking Stock of Automated Decision-Making in the EU' (AlgorithmWatch 2019) <https://algorithmwatch.org/en/wp-content/uploads/2019/02/Automating_Society_Report_2019.pdf> accessed 22 May 2024.

[20] Nicolò Pagan and others, 'A Classification of Feedback Loops and Their Relation to Biases in Automated Decision-Making Systems', *Equity and Access in Algorithms, Mechanisms, and Optimization* (ACM 2023) <https://dl.acm.org/doi/10.1145/3617694.3623227> accessed 21 July 2024.

Subsequently, attention will be directed toward a specific category of data within the scoring paradigm, i.e. biometric data. The decision to underscore this distinct classification of information emanated from its uniqueness and the consequential implications it harbours for privacy and data protection frameworks. The forthcoming assessment endeavours to appraise the intersections of these scoring mechanisms with fundamental rights, thus ensuring a complete understanding of their ramifications upon individuals and society at large. As a matter of fact, notwithstanding the enormous advantages, in the realm of disruptive technologies AI systems present substantial risks, thereby engendering a diverse array of legal challenges.[21]

Through manipulation and biases, these practices have an extensive potential to inflict unforeseeable harm to individuals' lives.[22] To exacerbate the situation, these processes often operate opaquely, with individuals potentially unaware of being profiled or lacking a comprehensive understanding of the involved mechanisms.[23] As it will be further discussed, these systems could lead to violations of essential human rights such as dignity and self-determination, privacy, and personal data protection, as well as non-discrimination, consumer rights and freedom of expression.[24]

2.2.1 Credit Scoring

Credit scoring is commonly recognised as a mathematical and statistical procedure utilised to forecast an individual's creditworthiness, which relies on an algorithmic examination of diverse information and data of the individual.[25] Initially, data are collected to establish a user outline, followed by an automated

[21] McLean and others (n 4).

[22] Martin Ebers, 'Chapter 2: Regulating AI and Robotics: Ethical and Legal Challenges' [2019] SSRN Electronic Journal <https://www.ssrn.com/abstract=3392379> accessed 21 July 2024.

[23] Article 29 Data Protection Working Party, 'Guidelines on automated individual decision-making and profiling for the purposes of regulation 2016/679' (2018) <https://ec.europa.eu/newsroom/article29/items/612053/en> accessed 19 March 2024.

[24] Martin Ebers and others, 'The European Commission's Proposal for an Artificial Intelligence Act—A Critical Assessment by Members of the Robotics and AI Law Society (RAILS)' (2021) 4 J 589.

[25] Boris Paal, 'Case Note: Article 22 GDPR: Credit Scoring Before the CJEU' (2023) 4 Global Privacy Law Review 127.

decision to either accept or reject the request based on the individual's risk profile analysed by the software. This evaluation is used to predict the likelihood of meeting credit obligations and ultimately informs the decision on whether to grant or deny loans.[26] Furthermore, within certain national systems, for instance the Italian one, electricity and gas supply companies wield this potent tool: before activating a new utility service, it must undergo assessment via an automated credit scoring process akin to that of credit institutions.[27]

Banks and FinTech companies are revolutionising credit decision-making by leveraging AI and machine learning.[28] These companies utilise innovative systems to evaluate creditworthiness, incorporating unconventional data sources such as educational backgrounds, living areas or ethnicities.[29] The rationale behind employing these tools stems from empirical observations indicating the tendency of human behaviours to recur.[30] By utilising this sequential characteristic, it is deemed feasible to compute the likelihood of specific conducts repeating through a mathematical process integrated into the algorithm.[31] AI-driven scoring methods open doors for extending credit to individuals whose creditworthiness may not be adequately represented by traditional factors, such as credit history and income. However, it also introduces fresh concerns about regulatory frameworks that may struggle to manage these developments effectively.[32] Specifically, the implication revolves around the latent risk of generating discriminatory outcomes when employing alternative data sources. The process may pose challenges when it

[26] Juliette Faivre, 'The AI Act: Towards Global Effects?' [2023] SSRN Electronic Journal <https://www.ssrn.com/abstract=4514993> accessed 23 February 2024.

[27] See, for example, the Italian information system referred to in Art. 117 of the Code in Legislative Decree No. 196/2003, which may be accessed by the persons participating in the prevention system referred to in para. 5 of Article 30-ter of Legislative Decree No. 141/2010 (among others: entities authorised to carry out sales activities to end customers of electricity and natural gas).

[28] Katja Langenbucher, 'Responsible A.I.-Based Credit Scoring – A Legal Framework' (2020) 31 European Business Law Review 527.

[29] Crystal S Yang and Will Dobbie, 'EQUAL PROTECTION UNDER ALGORITHMS: A NEW STATISTICAL AND LEGAL FRAMEWORK' (2020) 119 Michigan Law Review 291.

[30] Langenbucher (n 28).

[31] Elena Falletti, 'Credit Scoring Under Scrutiny by the Court of Justice of the European Union: Brief Remarks on the "SCHUFA Decision"' [2024] SSRN Electronic Journal <https://www.ssrn.com/abstract=4726282> accessed 16 March 2024.

[32] Langenbucher and Corcoran (n 11).

systematically disadvantages specific groups or individuals and may constitute discriminatory practices legally characterised by the unjust or disparate treatment of individuals or groups based on protected attributes.[33]

2.2.2 Social scoring

As delineated in Recital 31 of the AIA, social scoring refers to the process by which AI systems assess or categorise individuals or groups by analysing various data points concerning their social interactions, behaviours, and personality traits across different contexts, either "*known, inferred, or predicted*", over specific periods.[34] As a general understanding, every individual's conduct, demeanour, and societal engagements undergo assessment through a designated point-based system within their community. A superior score can unveil remarkable opportunities and distinct privileges, whereas a lower rating may lead to social alienation, bringing about both immediate and lasting repercussions.[35] One of the most renowned instances of social scoring is exemplified by the Social Credit System introduced by the Chinese government, employed for monitoring citizens, entities, and businesses via a sophisticated framework of surveillance and evaluation, entwined with mechanisms for reward and sanction.[36] In October 2016, the British dystopian TV series Black Mirror featured an episode titled "*Nosedive*", which perfectly reflected a concrete example of social scoring. Within this narrative, citizens utilise their mobile devices to rate each other on a 5-star scale following every social interaction, with each individual's average score being transparent to others on a platform.[37] In this societal paradigm, any manifestation of divergence in opinion culminates in diminished ratings, thereby initiating a descent into social ostracism and

---

[33] Xavier Ferrer and others, 'Bias and Discrimination in AI: A Cross-Disciplinary Perspective' (2021) 40 IEEE Technology and Society Magazine 72.

[34] Recital 31 AIA (n 9).

[35] Paul F Langer, 'Lessons from China - The Formation of a Social Credit System: Profiling, Reputation Scoring, Social Engineering', *The 21st Annual International Conference on Digital Government Research* (ACM 2020) <https://dl.acm.org/doi/10.1145/3396956.3396962> accessed 21 July 2024.

[36] Jing Wang and others, 'Envisioning a Credit Society: Social Credit Systems and the Institutionalization of Moral Standards in China' (2023) 45 Media, Culture & Society 451.

[37] Nicolas Kayser-Bril, 'Personal Scoring in the EU: Not Quite Black Mirror yet, at Least If You're Rich' (*Algorithm Watch*) <https://algorithmwatch.org/en/personal-scoring-in-the-eu-not-quite-black-mirror-yet-at-least-if-youre-rich/> accessed 20 April 2024.

eventual ruin. The examination of this fictional scenario reveals several potential violations of fundamental rights. Firstly, the right to privacy is compromised due to the public exposure of personal interactions and opinions, which subjects individuals to scrutiny and potential misuse of their private information. Secondly, the system's encouragement of conformity and penalisation of dissent impinges upon the freedom of expression, as individuals may be deterred from voicing divergent opinions. Furthermore, the right to non-discrimination is at risk, as individuals with lower ratings may be denied access to certain opportunities.

The underlying principle of social scoring posits that socially conscientious conduct merits recognition and reward, as it contributes to the improvement and safety of society.[38] Notwithstanding the noble objective, inquiries arise regarding the legitimacy of certain extents of surveillance and the associated sacrifices for collective welfare.[39] Respecting human dignity, which entails the belief that each individual holds an inherent value, is imperative and must not be eroded or jeopardised by external forces.[40] All individuals must be treated with the reverence they deserve as moral agents, rather than as commodities to be categorised, evaluated, or influenced. The development of this process does not seem to prioritise the supporting and safeguarding of the physical and psychological well-being of humans, nor their individual and cultural identities.[41] In addition, further challenges to the notion of individual autonomy, particularly within the framework of the right to freedom of expression, as already mentioned, are posed. The mechanism merely relies on statistical associations rather than causal links, leading to a conflict between correlation and causation.[42] This phenomenon, termed in the literature as 'data determinism',

---

[38] Langer (n 35).

[39] Lianrui Jia, 'Unpacking China's Social Credit System: Informatization, Regulatory Framework, and Market Dynamics' (2020) 45 Canadian Journal of Communication 113.

[40] Carmen Loefflad and Jens Grossklags, 'How the Types of Consequences in Social Scoring Systems Shape People's Perceptions and Behavioral Reactions' *The 2024 ACM Conference on Fairness, Accountability, and Transparency* (ACM 2024) <https://dl.acm.org/doi/10.1145/3630106.3658986> accessed 21 July 2024.

[41] High-level Expert Group on Artificial Intelligence, 'Ethics Guidelines for Trustworthy AI' (2019) < https://www.aepd.es/sites/default/files/2019-09/ai-definition.pdf> accessed 23 March 2024.

[42] Gernot Rieder and Judith Simon, 'Big Data: A New Empiricism and its Epistemic and Socio-Political Consequences' in Wolfgang Pietsch, Jörg Wernecke and Maximilian Ott

entails individuals being evaluated based on statistical inferences derived from their data, potentially undermining their autonomy in self-representation.[43] As a consequence, the processes tend to rigidify complex concepts, thereby eliminating fluidity and contestability, potentially infringing upon individuals' autonomy, and fostering deeper discrimination.[44]

Numerous international and national authorities have articulated their concerns on this matter and taken a definitive stance, such as UNESCO, which in its Recommendation on the Ethics of AI included a provision stating that AI systems ought not to be utilised for the objectives of social scoring or mass surveillance,[45] or the Italian Data Protection Authority, which underscored the potential adverse legal ramifications of a theoretical 'points-based citizenship' system on the rights and liberties of individuals, particularly those who are most vulnerable.[46]

2.3 The Interplay between Biometric Data and Scoring

As already anticipated, this area of scrutiny does not pertain to the analysis of a distinct type of scoring in isolation. Rather, it entails a broader examination of the potential integration of biometric data within established scoring systems mentioned earlier, as well as its application in diverse fields of practice. In the interest of this research, we consider the phenomenon of scoring through biometric data as entailing the assignment of scores based also on an individual's biometric information, intending to determine eligibility for various privileges as seen above, being them e.g., credit or employment opportunities.

(eds), *Berechenbarkeit der Welt?* (Springer Fachmedien Wiesbaden 2017) <http://link.springer.com/10.1007/978-3-658-12153-2_4> accessed 21 July 2024.

[43] Evgeni Aizenberg and Jeroen Van Den Hoven, 'Designing for Human Rights in AI' (2020) 7 Big Data & Society 205395172094956.

[44] Monique Mann and Tobias Matzner, 'Challenging Algorithmic Profiling: The Limits of Data Protection and Anti-Discrimination in Responding to Emergent Discrimination' (2019) 6 Big Data & Society 205395171989580.

[45] UNESCO, 'Recommendation on the Ethics of Artificial Intelligence' [2021] <https://unesdoc.unesco.org/ark:/48223/pf0000381137> accessed 16 March 2024.

[46] Garante per la Protezione dei Dati Personali, '"Cittadinanza a punti": Garante privacy ha avviato tre istruttorie. Preoccupanti i meccanismi di scoring che premiano i cittadini "virtuosi"' [2022]

<https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9778361> accessed 16 March 2024.

It is also imperative to first establish a unified definition of this class of data, starting with that adopted in the AIA and duplicated from the GDPR, which describes them as

> *personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data*.[47]

A concrete example of the use of biometric data can be found in Facial Recognition Technology, which involves capturing a facial image, creating its digital representation and storing it in a biometric database. Individuals are then identified by comparing the stored representation with other templates in the database.[48]

However, it is contended that the definition provided in the GDPR, and subsequently in the AIA, omits a significant category of data, which a European Parliament Study has defined as 'biometric-based data'.[49] Even if their processing is not prohibited under Art. 9 GDPR and they do not "*allow or confirm*" the identification of an individual, such as pulse rate, body temperature and non-distinct facial expressions or vocal cues, they may encompass serious risks.[50] As a matter of fact, this kind of information, which is not officially protected under any EU legislation, could unveil patterns in individuals' actions, shedding light on their identity, thoughts and potential future actions and, through machine learning techniques, it can identify, influence, incentivise and penalise.[51] Consequently, for the purposes of this study, which seeks to underscore the safeguards associated with scoring systems, it is asserted that

---

[47] Art. 4(14) GDPR (n 8).

[48] European Data Protection Board, 'Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement' (2023) <https://www.edpb.europa.eu/system/files/2023-05/edpb_guidelines_202304_frtlawenforcement_v2_en.pdf> accessed 21 July 2024.

[49] European Parliament. Directorate General for Internal Policies., *Biometric Recognition and Behavioural Detection.* (Publications Office 2021) <https://www.europarl.europa.eu/RegData/etudes/STUD/2021/696968/IPOL_STU(2021)696968_EN.pdf> accessed 20 February 2024.

[50] ibid.

[51] Quantumrun Foresight, 'Biometric scoring: Behavioral biometrics might verify identities more accurately' [2023] <https://www.quantumrun.com/insight/biometric-scoring-behavioral-biometrics-might-verify-identities-more-accurately> accessed 16 March 2024.

this broader definition should be taken into account. This approach will facilitate a more comprehensive analysis of the rights and requirements implicated.

To better circumvent the area of interest this part will now furnish two hypothetical instances illustrating the interaction between biometric-based data and AI scoring systems. The initial case under examination involves the hypothesis of a scoring algorithm employed by a lender to assess creditworthiness through analysis of speech patterns, like a regional or class-linked accent, or facial expressions.[52] As previously stated, the processing of these characteristics is not expressly prohibited by Art. 9 GDPR, since they cannot "*uniquely identify*" the data subject,[53] and could therefore theoretically escape the Article's stricter provisions and lead to unfair decisions. The second example relates to an already mentioned situation, i.e. to the job market and candidate assessment, leveraging biometric and biometric-based data, such as the voice and its cues or facial expression, to streamline the hiring process efficiently at scale. The AI system can facilitate applicant evaluation from the initial phase to skill-based screening, enhancing the efficiency of vendor management systems and enabling biometric scoring, on several characteristics, for rapid candidate shortlisting.[54]

The scoring methodology delineated in the preceding examples appears to intersect both with the previously mentioned concept of creditworthiness and, to some extent, with the social one. However, the distinctiveness of this approach stems from the utilisation of a unique category of information, specifically a biometric-based one. Using these highly invasive practices enables the precise determination of each individual's risk profile and could help

[52] Alex Lawrence-Archer and Ravi Naik, 'Effective Protection against AI Harm' (AWO Agency 2023) <https://www.awo.agency/blog/awo-analysis-shows-gaps-in-effective-protection-from-ai-harms/> accessed 17 March 2024.

[53] European Data Protection Board, 'Guidelines 3/2019 on Processing of Personal Data through Video Devices' (2020)<https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201903_video_devices_en_0.pdf> accessed 17 March 2024, para 76.

[54] 'The Opportunity For AI In Vendor Management Systems' (*Simplify beyond the vms*, 2021) <https://www.simplifyvms.com/resources/blogs/ai-in-recruitment/the-opportunity-for-ai-in-vendor-management-systems/> accessed 17 March 2024.

organisations make well-informed decisions, potentially resulting in practices such as price discrimination.[55]

This first chapter has offered a concise definition of scoring and scoring systems, incorporating both existing and hypothetical examples, along with their implications for fundamental rights. Subsequently, we have concentrated on a specific category of data and the potential issue inherent in its definition, which appears insufficient in scope and protection.

In the forthcoming sections, the dual issue between biometric and biometric-based data will be examined, focusing on the potential existence of a loophole within EU legislation regarding scoring systems involving this category of information, as well as the adequacy of the existing definition(s) of biometric data.

[55] Frederik Zuiderveen Borgesius and Joost Poort, 'Online Price Discrimination and EU Data Privacy Law' (2017) 40 Journal of Consumer Policy 347.

3. The Interaction between the GDPR and the AIA on Scoring

3.1 Scoring Systems in the GDPR

In this section, we will examine the scope and implications of scoring systems in the GDPR. Specifically, the analysis aims to first elucidate (whether there are) provisions within this framework that pertain to AI-based scoring mechanisms and subsequently how personal data, and specifically biometric ones, are safeguarded, aligning with the fundamental right enshrined in Art. 16 TFEU and 8 CFREU.[56]

3.1.1 SCHUFA and Art. 22(1) GDPR

The GDPR does not explicitly reference the concept of scoring neither in its articles nor in the recitals that precede them. Nonetheless, a recent landmark judgment delivered by the ECJ has significantly clarified the regulatory landscape.[57] The case entailed judicial proceedings between an individual, the German Land Hessen and SCHUFA, a private company which, through mathematical-statistical procedures, furnishes its contractual partners with insights into consumer's creditworthiness. In this instance, SCHUFA provided a credit score for the applicant, serving as the rationale for rejecting the credit application she had made. The individual requested SCHUFA to disclose the personal data held, based on the right to access, granted by Art. 15(1)(h) GDPR, and the removal of purportedly erroneous information. In reply, the agency provided the applicant with her credit score and a general overview of the methodologies employed in the calculation. However, levering trade secrecy, SCHUFA declined to divulge the factors considered or their respective weights. Additionally, it clarified that it solely disseminated information to its contractual affiliates, who ultimately made the decision. In light of the circumstances, the German Court opted to stay the proceedings and seek clarification from the ECJ regarding the interpretation of Art. 22(1) GDPR, which states that "*The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her*".[58] Specifically,

[56] Cfr. Alessandra Silveira, 'Automated Individual Decision-Making and Profiling [on Case C-634/21 - SCHUFA (Scoring)]' (2023) 8 UNIO – EU Law Journal 74.

[57] Case C-634/21 *SCHUFA Holding (Scoring)* [2023] ECLI:EU:C:2023:957.

[58] Art. 22(1) GDPR.

it questioned whether the automated generation of a probability value concerning a data subject's ability to service a loan, which is transmitted by one controller to another and heavily influences decisions regarding contractual relationships, constitutes a decision solely based on automated processing with significant legal or similar effects on the data subject.[59]

The ECJ's judgment delineated three fundamental conditions for the application of Art. 22(1) GDPR. Firstly, there must be a decision significantly affecting the individual. Secondly, this decision must rely exclusively on automated processing, including profiling.[60] Lastly, it must lead to legal effects or similarly significant consequences for the individual. Following the earlier opinion of Advocate General (AG) Pikamäe, the ECJ asserted that the concept of a 'decision' is expansive and encompasses actions such as online credit application refusals or recruiting practices without human involvement, as clarified in Recital 71 of the GDPR. Additionally, activities akin to those of SCHUFA meet the GDPR's definition of "*profiling*,"[61] satisfying the second condition. Concerning the third one, the transmission of a probability value strongly influences the actions of the recipient, such as a bank's decision to grant a loan, thus meeting the requirement, as the probability value significantly impacts the data subject.[62]

Therefore, credit applicants are impacted throughout the assessment of their creditworthiness by the credit information agency, rather than solely during the final stage of credit denial, when the financial institution merely applies the evaluation outcome to the individual case.[63]

The interpretation established that AI-based scoring practices fall under the ambit of Art. 22(1) GDPR. Consequently, although not explicitly articulated, it can be inferred from the judgment that this piece of legislation regulates and partially defined AI-based (only credit?) scoring systems, which involve automated processing, including profiling. However, a thorough examination of

---

[59] SCHUFA, para 27.

[60] Cfr. Article 29 Data Protection Working Party (n 23): *To qualify as human involvement, the controller must ensure that any oversight of the decision is meaningful*.

[61] Art. 4(4) GDPR.

[62] SCHUFA, paras 43-50.

[63] SCHUFA, opinion of AG Pikamäe, para 43.

the obligations imposed on these practices under the Regulation is necessitated, including scrutiny of the provisions delineated in the remainder of the article.

3.1.2 ADM Exceptions, Rights, and Requirements under the GDPR

Notwithstanding the ECJ's interpretation of Art. 22(1) GDPR, the examination of paragraph (2) of the same article becomes imperative. This section stipulates exceptions to the prohibition outlined earlier, allowing for situations where the decision: (i) is "*objectively indispensable*"[64] for concluding or executing a contract between the data subject and a controller; (ii) is sanctioned by EU or Member State law; (iii) is predicated on the data subject's explicit consent. Notably, the exemptions of contractual necessity and explicit consent entail significant data protection risks, necessitating a high degree of individual control over personal data. Therefore, the prohibition delineated in Art. 22(1) may become ambiguous, particularly concerning contract and consent clauses that undermine the concept of autonomy of choice, to which individuals may adhere due to a lack of awareness or alternative options.[65]

In instances where the automated decision is founded upon a contract or the explicit consent of the data subject, pursuant to Art. 22(3) GDPR, the data controller is thus duty-bound to implement suitable measures to safeguard the rights and interests of the individual. These measures specifically entail affording the individual the right to request human intervention from the controller, to articulate their perspective, and to contest the decision. Recital 71 of the GDPR serves as a guiding principle for interpreting part of this provision, emphasising that adequate safeguards should encompass the entitlement to receive "*an explanation of the decision reached after such assessment and to challenge the decision*".[66] With regard to human intervention, it must be based on a thorough assessment of all relevant information, including any

---

[64] Case C-252/21 *Meta Platforms and Others* [2023] ECLI:EU:C:2023:537, paras 97-98.

[65] Alessandra Silveira, 'Profiling and Cybersecurity: A Perspective from Fundamental Rights' Protection in the EU' in Francisco António Carneiro Pacheco De Andrade, Pedro Miguel Fernandes Freitas and Joana Rita De Sousa Covelo De Abreu (eds), *Legal Developments on Cybersecurity and Related Fields*, vol 60 (Springer International Publishing 2024) <https://link.springer.com/10.1007/978-3-031-41820-4_15> accessed 3 May 2024.

[66] Recital 71 GDPR.

supplementary data provided by the subject, and must be conducted by an individual possessing the requisite authority and competence to alter the decision.[67]

Given their nature as ADM, data controllers are obligated under the GDPR to fulfil certain requirements to ensure fair and transparent processing of scoring practices. Of particular significance are Arts. 13(2)(f) and 15(1)(h) GDPR, which emphasise the importance of providing data subjects with comprehensive and transparent details regarding the reasoning behind the processing, as well as its implications, particularly in situations where the personal data has not been obtained directly from the data subject, as specified under Art. 14(2)(g). On the topic, the Council of Europe has issued guidelines, which could help with the interpretation of the legislation, stipulating that data subjects should have insight into the rationale behind the processing of their data which has led to either a positive or negative decision (e.g., on whether or not to grant a credit), rather than merely receiving information about the verdict itself.[68] A comprehensive understanding of these aspects enhances the effective exercise of fundamental safeguards such as the right to object and the right to lodge complaints with a competent authority.[69] As a matter of fact, only through the transparency requirement and a comprehensive understanding of how the decision was made and on what grounds, the data subjects will be able to contest a decision or articulate their viewpoints.[70]

3.1.3 ADM and Biometric-Based Data

The level of intrusiveness and the extent of privacy impact on individuals resulting from biometric data operations within a specific processing scenario may vary, contingent upon not only the employed techniques, but also the delineation of the processing, its inherent nature, scope or scale, and notably

[67] Article 29 Data Protection Working Party (n 23).

[68] Council of Europe, 'Explanatory Report to the Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data' (2018) <https://rm.coe.int/cets-223-explanatory-report-to-the-protocol-amending-the-convention-fo/16808ac91a> accessed 4 May 2024.

[69] ibid.

[70] Article 29 Data Protection Working Party (n 23).

the objectives being pursued.[71] Art. 22(4) GDPR stipulates that automated decisions cannot rely on special categories of personal data, including biometric ones, as specified in Art. 9(1). Nevertheless, the limitation imposed on exceptions to the prohibition of ADM is once more compromised by exemptions within the GDPR itself.[72] Specifically, these categories of personal data may be utilised for ADM provided the data subject has granted consent (Art. 9(2)(a)), or if such processing is necessary for reasons of substantial public interest based on an EU or Member State law (g), the latter possibly enhancing the potential for diverse national regulatory frameworks.[73] The legal basis for consent holds particular significance within the scoring context. Specifically, in scenarios involving automated decisions aimed at benefiting the data subject, such as during credit applications, obtaining freely given consent, as outlined in Art. 7(4) GDPR, may be comparatively easier to secure, since the individual is trying to pursue a personal interest, such as the grant of a loan.[74]

The risks associated with specific automated decision systems involving biometric data, such as systems designed to detect emotions, are considerable, notably encompassing cultural discrimination and stigmatisation due to algorithms often failing to account for cultural and societal variations.[75] This underscores the need for substantial, high-quality data to facilitate effective training, thereby improving result accuracy and mitigating biased decisions. As

---

[71] Spanish Data Protection Authority, 'Use of Biometric Data: Assessment from a Data Protection Perspective' (*AEPD*, 2022) <https://www.aepd.es/en/prensa-y-comunicacion/blog/biometric-data-assessment-from-a-data-protection-perspective> accessed 4 May 2024.

[72] Stephan Dreyer, Wolfgang Schulz, and Bertelsmann Stiftung, 'The General Data Protection Regulation and Automated Decision-Making: Will It Deliver?: Potentials and Limitations in Ensuring the Rights and Freedoms of Individuals, Groups and Society as a Whole' [2019] Discussion paper Ethics of Algorithms <https://www.bertelsmann-stiftung.de/doi/10.11586/2018018> accessed 4 May 2024.

[73] Isak Mendoza and Lee A Bygrave, 'The Right Not to Be Subject to Automated Decisions Based on Profiling' in Tatiana-Eleni Synodinou and others (eds), *EU Internet Law* (Springer International Publishing 2017) <http://link.springer.com/10.1007/978-3-319-64955-9_4> accessed 5 May 2024.

[74] Lee A Bygrave, 'Article 22 Automated Individual Decision-Making, Including Profiling' in Christopher Kuner and others (eds), *The EU General Data Protection Regulation (GDPR)* (Oxford University PressNew York 2020) <https://academic.oup.com/book/41324/chapter/352298561> accessed 5 May 2024.

[75] Simona Fanni, 'The Biometric Habeas Data in the Digital and Algorithmic Era in the European Union' (2023) 3 Latin American Journal of European Studies 18.

a result, the implementation of appropriate safeguards, such as human intervention, assumes critical importance.[76]

At this stage of the research, it is imperative to reaffirm the assertions articulated in Chapter 1, specifically regarding the definition of biometric data, and its inherent characteristic of "*confirming the unique identification"*, as in Art. 4(14) GDPR. The argument presented therein posits that the restrictive characterisation of biometric data solely as information uniquely identifying an individual is overly confined. As a result, there exists the possibility of evading the obligations outlined in Art. 22(4) GDPR, since data predicated on biometric attributes do not formally categorise as such under Art. 9 GDPR. Therefore, the exceptions outlined in Art. 22(2) would apply. For instance, 'legitimate' biometric data, such as voice or facial recognition, may be employed in the credit scoring process for a loan applicant solely with the explicit consent of the individual or in cases of substantial public interest. Conversely, when utilising biometric-derived and non-uniquely identifiable data, such as indistinct facial expressions or voice characteristics, the applicability extends to the contractual legal basis, providing a wider scope for implementation.

3.1.4 GDPR Wrap-up on Scoring

Despite the detailed reasoning provided by the ECJ in the SCHUFA case regarding the application of Art. 22 GDPR to credit scoring systems, gaps and uncertainties persist within the legislation. As demonstrated, AI-based credit evaluations by an agency amount to an automated decision which triggers the applicability of this cumbersome GDPR Article and necessitates safeguards to be implemented by the data controller. However, two principal issues have emerged. Firstly, it is questionable whether the interpretation of the ECJ can be applied *in extensu* to other fields where scoring methodologies are employed, such as the insurance sector or e-recruiting practices: are *decisions* what we encounter or alternative forms of outputs, such as computer-based *recommendations*, which then always require human intervention?[77] Secondly, notwithstanding the seemingly stringent provisions concerning special

[76] ibid.

[77] Peter Davis and Sebastian Felix Schwemer, 'Rethinking Decisions Under Article 22 of the GDPR: Implications for Semi-Automated Legal Decision-Making' [2023] SSRN Electronic Journal <https://www.ssrn.com/abstract=4478107> accessed 5 May 2024.

categories of data, thus biometric ones as well, there remains a potential for circumvention when considering biometric-derived data that do not meet the criteria stipulated in the Regulation.

The following section of this Chapter aims to look beyond the GDPR and explore the provisions on scoring within the AIA, which recently entered into force. Will this new legislation introduce more precise, and possibly stringent, requirements for AI-based scoring systems?

3.2 Scoring Systems in the AI Act

In the second part of this Chapter, the provisions delineated in the AIA concerning scoring practices will be analysed. As of the time of drafting, the Regulation has just entered into force and will apply from the 2nd of August 2026.

Similarly to the GDPR, the AIA embraces a risk-based framework, establishing prohibitions for AI systems linked with unacceptable risks and imposing several stringent requirements on those classified as high-risk. Conversely, AI systems deemed to present low or minimal risk encounter fewer restrictions. To address the hazards linked with high-risk AI systems, providers thereof are compelled to conform to the mandates delineated in Chapter 2 of the Regulation.[78]

In contrast to the analysis conducted thus far, the AIA explicitly address scoring systems, specifically the already described credit and social scoring. Consequently, the forthcoming section will delve into an examination of this legislation concerning these practices.

3.2.1 What Is Allowed: (not only) Credit Scoring as a High-Risk System

The AIA specifically governs the practice of credit scoring, by assigning it to the high-risk category. Point 5 of Annex III, referenced by Art. 6(2), enumerates high-risk systems, including those assessing eligibility for essential public assistance benefits and services, individual credit scores (excluding methodologies for detecting financial fraud), systems for evaluating and classifying emergency calls, and those intended for risk assessment and pricing

[78] Jonas Schuett, 'Risk Management in the Artificial Intelligence Act' [2023] European Journal of Risk Regulation 1.

in life and health insurance. Recital 55 elucidates that such AI systems might impact the access to resources and services crucial for human well-being and societal participation, such as essentials like housing or electricity, and may engender discriminatory effects. Hence, the imperative to classify them as high-risk. [79]

Considering the listing under the same category, the concise description alongside with the recital abovementioned, it is posited that not only do systems assessing creditworthiness fall within the scope of the scoring paradigm, but also the other methodologies may potentially belong to this classification. This inference arises from the shared characteristic wherein systems are employed for evaluation purposes, necessitating therefore the assignment of some form of score. Another domain where scoring methodologies may be applied, previously examined, pertains to systems designed for the recruitment or selection of individuals, particularly in assessing candidates. This too is recognised as carrying high inherent risks and has been included immediately preceding the point analysed.[80] In light of the delineated description, we also regard this as falling within the purview of scoring practices. Further substantiating our contention is the latter segment of Art. 6(2)(a), which asserts that any AI system engaging in profiling of individuals shall invariably be deemed high-risk. Drawing upon our examination of the SCHUFA case, wherein credit scoring practices were delineated as constituting profiling endeavours, it follows that all forms of scoring methodologies might be construed as falling within the high-risk classification.[81] However, as previously noted, given the potential applicability of SCHUFA solely to creditworthiness practices and the absence of further interpretation or case law, this reasoning may appear somewhat tenuous.

Given their high-risk 'nature', Title III stipulates that these systems are subject to various *ex ante* and *ex post* conformity assessments. The requirements encompass provisions such as the establishment of a risk management system, comprehensive technical documentation, cybersecurity

[79] Recital 37, Art. 6(2), Annex III point 5 AIA.

[80] Annex III point 4 AIA.

[81] Art. 6(2)(a) AIA; SCHUFA para 47.

protocols, and notification procedures. The intricate nature of the substantive scope of the AIA poses significant challenges. Navigating and implementing its provisions may prove ambiguous for both regulatory authorities and stakeholders involved in the development and deployment of AI systems.[82] In the interest of brevity, the discussion will concentrate on the obligations pertaining to the protection of personal data and its specific categories, as well as data subjects – them being data governance, transparency and human oversight - and their link to the GDPR.

Art. 10 AIA delineates provisions regarding data governance in the development of high-risk AI systems utilising data training techniques. It mandated that such systems must be based on training, validation, and testing datasets meeting defined quality criteria. If we focus on biometric data, it is specified that providers may exceptionally process special categories of data, as defined in Art. 9(1) GDPR, for bias detection and correction purposes. However, such processing must adhere to stringent safeguards to protect fundamental rights and freedoms, including technical limitations, security measures, access controls, and deletion protocols.[83]

AI systems may lead to discrimination due to various factors. One of them is imbalanced training data, as seen in loan repayment prediction systems skewed, for example, towards male borrowers from certain ethnic backgrounds due to historical data patterns.[84] Addressing this issue may require adjusting data subsets, although careful consideration of potential impacts on over- or under-represented populations is essential. Art. 10 AIA seems to align with the privacy by design and by default principle outlined in Art. 25 GDPR. [85] It mandates the development of AI systems to consider essential aspects such as

---

[82] Jérôme De Cooman, 'Humpty Dumpty and High-Risk AI Systems: The Ratione Materiae Dimension of the Proposal for an EU Artificial Intelligence Act' [2022] Market and Competition Law Review 49.

[83] Art.10(5) AIA.

[84] Alister Pearson, 'How to Use AI and Personal Data Appropriately and Lawfully' (Information Commissioner's Office (UK) 2022) <https://policycommons.net/artifacts/3534587/how-to-use-ai-and-personal-data-appropriately-and-lawfully/4335800/> accessed 12 May 2024.

[85] Federica Pucarelli and Maddalena Collini, 'Intelligenza Artificiale e Protezione Dei Dati: Una Convivenza Possibile?' (*Stefanelli&Stefanelli*, 2023) <https://www.studiolegalestefanelli.it/it/approfondimenti/intelligenza-artificiale-e-protezione-dei-dati-una-convivenza-possibile/> accessed 12 May 2024.

data collection, processing operations including cleansing and aggregation, and preliminary assessments of data adequacy. This method mirrors the conceptual approach of prior mapping, design, and analysis, serving as a guide for the data protection framework.[86]

Art. 13 AIA mandates transparency requirements obligations for high-risk AI systems, ensuring users can interpret and utilise system outputs effectively. Although not explicitly addressing the intersection with the GDPR, it aligns logically with its transparency principle enshrined in Art. 5 and outlined in Arts. 13 and 14, where it requires data controllers to inform data subjects about data handling specifics and associated risks.[87]

Art. 14 AIA focuses on the crucial aspect of human oversight in the development and design of high-risk systems. It emphasises the necessity for these systems to be constructed with features that facilitate effective monitoring by individuals, aided by suitable human-machine tools, throughout the AI system's operation. Furthermore, of particular significance is paragraph (4)(b), which underscores the importance of recognising and guarding against 'automation bias' in high-risk AI systems, especially those providing information or recommendations for human decision-making. A parallel may be drawn between this provision and Art. 22 GDPR: the GDPR provision exhibits a wider purview compared to Art. 14 AIA in that it encompasses processing activities extending beyond the realm of high-risk AI applications. Conversely, Art. 14 AIA expands its reach beyond the confines of Art. 22 GDPR by mandating human oversight not only in the processing of personal data, but also in safeguarding health, safety, and fundamental rights beyond the scope of data protection.[88]

As observed, numerous requirements are imposed on providers and deployers of high-risk AI systems concerning data protection, with significant connections to the GDPR. Based on our understanding of the legislation, these

---

[86] ibid.

[87] Balint Gyevnar, Nick Ferguson and Burkhard Schafer, 'Bridging the Transparency Gap: What Can Explainable AI Learn From the AI Act?' <https://arxiv.org/abs/2302.10766> accessed 12 May 2024.

[88] Claes G Granmar, 'AI-Based Decision-Making and the Human Oversight Requirement Under the AI Act' in Eduardo Gill-Pedro and Andreas Moberg (eds), *YSEC Yearbook of Socio-Economic Constitutions 2023*, vol 2023 (Springer Nature Switzerland 2024) <https://link.springer.com/10.1007/16495_2024_68> accessed 7 May 2024.

obligations extend to scoring methodologies. Regarding special categories of data, so 'proper' biometric data as delineated in Art. 9 GDPR, stricter compliance standards apply. Nonetheless, thus far, no explicit mention of scoring utilising what we have framed as biometric-based data has been identified, therefore the issue defined in the previous section is still open.

3.2.2 What Is Not Allowed: Social Scoring

Art. 5 AIA enumerates prohibited AI practices. Paragraph 1(c) specifically pertains to AI systems designed *"for the evaluation or classification of natural persons or groups of persons over a certain period of time based on their social behaviour or known, inferred or predicted personal or personality characteristics",* with resultant social scoring leading to adverse treatment. This prohibition, as elucidated in Recital 31, applies to both public and private entities, despite an earlier iteration of the Regulation solely referencing public actors.[89] As outlined in Chapter 1, the score could depend on daily activities undertaken by the citizen. For instance, adherence to public health protocols, such as compliance with quarantine directives or receiving vaccinations, could increase one's score.[90] Given the expansive language of the provision, concerns are emerging regarding the potential for circumventing the prohibition and implementing systems which are 'only' classified as high-risk ones, such as those allocating public assistance benefits, which aggregate a broad spectrum of personal and sensitive data.[91] Indeed, discerning whether a system is causally linked to a particular outcome may prove challenging, particularly in instances where the social contexts diverge from those in which the data was initially produced or collected, or whether the treatment is deemed unjustified or disproportionate. This ambiguity may allow private or public entities to utilise the system and argue that the scoring was not a decisive factor.[92] Another aspect that may contribute to confusion pertains to the connection with other

[89] Art. 5(1)(c) and Recital 31 AIA.

[90] Janos Meszaros, Jusaku Minari and Isabelle Huys, 'The Future Regulation of Artificial Intelligence Systems in Healthcare Services and Medical Research in the European Union' (2022) 13 Frontiers in Genetics 927721.

[91] 'EU: Artificial Intelligence Regulation Should Ban Social Scoring' (*Human Rights Watch*, 2023) <https://www.hrw.org/news/2023/10/09/eu-artificial-intelligence-regulation-should-ban-social-scoring> accessed 12 May 2024.

[92] Ebers and others (n 24).

scoring methodologies. Given that an increasing amount of information pertaining to our "social behaviour"[93] may be utilised to evaluate our creditworthiness, can it be posited that credit scoring when employing such data, could constitute a subset of social scoring? Where is the demarcation line drawn? If these provisions were to apply to AI credit scoring, the utilisation of alternative data for generating credit scores could be construed as employing data in a context "unrelated to the contexts in which the data was originally generated or collected".[94] Consequently, this would imply that social behaviour and personal or personality characteristics cannot be factored into scoring methodologies.[95] What also remains ambiguous and does not find a proper definition in the AIA is the actual delineation of "personal and personality characteristics", whose evaluation or classification is prohibited together with "social behaviour" in Art. 5(1) AIA. This warrants thorough examination, potentially encompassing associations with biometric or biometric-based data.

3.3 Any Room for Circumvention?

As demonstrated, the legal landscape is intricate and open to interpretation, necessitating a concise overview. Credit scoring practices have been categorised as ADM practices, thereby falling within the purview of Art. 22 GDPR, given they meet three fundamental criteria (being a decision, based on profiling, and causing individual consequences). Expansive interpretation of the ECJ decision suggests this could extend to various scoring methodologies. However, within our focus on biometric-based data, it appears that compliance requirements are easily evaded. Indeed, 'genuine' biometric data could be subject to scoring practices either through individual consent or lawful authorisation. Additionally, biometric-based data falling outside the scope of Art. 9 GDPR could also be subject to scoring via contractual obligations. Turning to the AIA, specific mandates are imposed on systems assessing individuals' creditworthiness and those influencing access to vital services like housing or electricity. Furthermore, while social scoring is proscribed, uncertainties persist regarding the limitations of this prohibition. Finally, the concept of personality traits appears to intersect

[93] Art. 5(1)(c) AIA.

[94] Art. 5(1)(c)(i) AIA.

[95] Langenbucher and Corcoran (n 11).

with our understanding of biometric-based data, as indicated by Recital 16 AIA and the definition of biometric categorisation.[96] This will serve as the focal point for our forthcoming third and final Chapter.

[96] Recital 16 AIA states: "The notion of 'biometric categorisation' referred to in this Regulation should be defined as assigning natural persons to specific categories on the basis of their *biometric data*. Such specific categories can relate to aspects such as sex, age, hair colour, eye colour, tattoos, *behavioural or personality traits*, language, religion, membership of a national minority, sexual or political orientation".

4. Scoring through Biometric Data: Comparative Analysis, Examples and Legal Challenges

After having considered how scoring practices are regulated within the GDPR and AIA, this Chapter endeavours to conduct a thorough analysis to study whether scoring systems involving specifically biometric and biometric-based data (could) exist. To reach a definitive conclusion, the process will begin by examining the concepts of biometric categorisation and personality traits and characteristics under the AIA, which appear to be the most relevant for the scope of this research, in order to find potential similarities with what we have defined as biometric-based data and to assess the applicability of specific parameters to the subject matter.

Following this, concrete and existent examples from within the Union will be presented, and the analysis will then extend to consider practices in non-EU countries. The discussion will culminate in an exploration of the potential legal challenges inherent in this phenomenon.

4.1 Biometric Categorisation and the Concept of Personality Traits

The most pertinent and specific concept related to scoring through biometric data within the AIA is biometric categorisation. However, this process involves assigning individuals to specific categories based on their biometric data,[97] without conducting a proper evaluation or classification as typically seen in scoring processes. Of particular interest to this research is what is included under the possible categories, i.e. "*behavioural or personality traits"*.[98] A similar concept is articulated in the definition of social scoring, as discussed in Chapter 2, which prohibits the evaluation or classification of individuals based on their "*personality characteristics".*[99] The distinction lies in the process: in biometric categorisation, 'proper' biometric data are used to group individuals according to their personality traits.[100] Conversely, in social scoring practices, "*known,*

[97] Recital 16 AIA.

[98] ibid.

[99] Art. 5(1)(c) AIA.

[100] Isabelle Hupont and others, 'The Landscape of Facial Processing Applications in the Context of the European AI Act and the Development of Trustworthy Systems' (2022) 12 Scientific Reports 10688.

inferred, or predicted personal or personality characteristics"[101] are used as the input to generate a social score as the output.[102] What remains undefined is the precise definition of "*personal or personality characteristics*" and the potential for these to constitute biometric or biometric-based data, given their inclusion in the definition of biometric categorisation. Its interpretation can yield significant implications: if "*personal or personality characteristics*" are construed to encompass types of data related to an individual's "*behavioural"* features able to personally recognise them, this would link to the definition of biometric data under Art. 4(14) GDPR,[103] thereby prohibiting scoring through biometric data, as a subset of social scoring. Notwithstanding their dynamicity, behavioural data are unique to each person and permanent.[104] Typical behavioural data include both offline and online conducts, such as signatures, analysis of keystroke, gait, movement patterns.[105]

Should this concept be broadly interpreted to include behavioural characteristics that do not identify the person, the interdiction would be even more extensive. Nevertheless, in the absence of a specific definition and considering that biometric categorisation – directly relevant to our primary focus – is mostly classified as a high-risk practice rather than being proscribed (notwithstanding the inaccuracy and bias issues), such data may still be utilised for scoring practices under the conditions previously outlined.

In summary, the concept in the AIA most closely associated with scoring through biometric data is biometric categorisation, considered high-risk practice, thus permissible. This involves assessing "*behavioural or personality traits"*, which seems to align with the definition of biometric data in Art. 4(14)

---

[101] Art. 5(1)(c) AIA.

[102] Loefflad and Grossklags (n 40).

[103] Art. 4(14) GDPR states: 'biometric data' means personal data resulting from specific technical processing relating to the physical, physio- logical or *behavioural* characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data.

[104] Ján Matejka, Alžběta Krausová and Vojen Güttler, *Biometric Data and Its Specific Legal Protection* (Institute of State and Law of the Czech Academy of Sciences 2020).

[105] Article 29 Data Protection Working Party, 'Opinion 3/2012 on developments in biometric technologies' (2012) <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2012/wp193_en.pdf> accessed 22 July 2024.

GDPR. However, the AIA explicitly prohibits social scoring, which includes evaluation based on "*personal or personality characteristics".* Therefore, it is debatable whether (i) "*personal or personality characteristics"* can be equated with "*behavioural or personality traits"* under the definition of biometric categorisation and thus linked to the definition of biometric data under Art. 4(14); whether (ii) it has a broader meaning that also encompasses what we define as biometric-based data; or whether (iii) there is no link at all and "*personal or personality characteristics"* cannot be associated with biometric data.

To gain a clearer understanding of this unresolved issue, prior to any future (and needed) interpretation by the CJEU, it may be beneficial to examine concrete examples planned or already in place before the AIA.

4.2 The Concrete Use of Biometric Data in Scoring Systems

The following section aims to examine existing (or already planned) scenarios of particularly invasive scoring practices and the possible usage of biometric data. This analysis will evaluate the compatibility of these examples with the GDPR and AIA, to identify any potential loophole in the legislation.

4.2.1 Existing Scoring Examples in the EU

The *Dutch Systeem Risico Indicatie* (SyRI) is a notable example of a scoring system, which was halted in 2020 by the Court of the Hague for violating Art. 8 of the European Convention on Human Rights.[106] This risk-scoring algorithm was designed to predict fraud and non-compliance among individual welfare recipients in social security and income-dependent schemes, using risk indicators derived from historical data.[107] Due to its focus on poorer neighbourhoods, the system was criticised as implementing a "*surveillance state for the poor*".[108] The SUWI Act, which regulated SyRI, allowed the Dutch tax authority to process any data held by the administration or government bodies,

[106] Rechtbank Den Haag, ECLI:NL:RBDHA:2020:1878 [2020].

[107] 'The Siry Case Netherlands, Court of the Hague: Systeem Risico Indicatie (SyRI)' (*AI Taxadmin.EU*) <https://www.uantwerpen.be/en/projects/aitax/publications/syri/> accessed 22 May 2024.

[108] Philip Alston, 'The Netherlands Is Building a Surveillance State for the Poor, Says UN Rights Expert' (United Nations Human Rights 2019) <https://www.ohchr.org/en/press-releases/2019/10/netherlands-building-surveillance-state-poor-says-un-rights-expert> accessed 22 May 2024.

including health data, belonging to the special categories of data under Art. 9 GDPR.[109] The algorithm analysed past cases of both compliant and fraudulent welfare recipients to identify risk factors and develop a scoring grid, which enabled the flagging of certain individuals for additional audits by human officials.[110] Despite the legislation's goal, the Court highlighted the algorithm's potential for discrimination and cited the lack of transparency and sufficient safeguards for citizens, referencing the principles enshrined in Art. 5 GDPR.[111] Notwithstanding its intrusive nature, this scoring system did not utilise any kind of biometric data, thereby the applicability to the scope of this research is limited.

Several other AI-based scoring practices, either currently in use or planned within the EU, condense various personal data inputs into a single number or measure, enabling algorithms to make decisions. Examples include determining eligibility for housing support and social benefits through the analysis of several databases in Trelleborg (Sweden),[112] and assessing continued suitability for subsidised electricity prices through income and rent data as happened in Spain with the BOSCO program.[113]

From a superficial point of view, these systems, when compliant with all the GDPR requirements previously seen, seem also to be in scope and not prohibited with the upcoming AIA. However, as above, no use of biometric data has been detected.

An initiative that might need deeper analysis instead is the Horizon 2020-funded research project iBorderCTRL.[114] This system is intended to screen non-EU nationals seeking to cross the EU border. In the first phase, an online

[109] Rechtbank Den Haag (n 106).

[110] ibid.

[111] Naomi Appelman, Ronan Ó Fathaigh, and van Hoboken, Joris, 'Social Welfare, Risk Profiling and Fundamental Rights: The Case of SyRI in the Netherlands' [2021] JIPITEC 257.

[112] Kayser-Bril (n 37).

[113] Eva Belmonte, 'La Aplicación Del Bono Social Del Gobierno Niega La Ayuda a Personas Que Tienen Derecho a Ella' (*CIVIO*, 2019) <https://civio.es/tu-derecho-a-saber/2019/05/16/la-aplicacion-del-bono-social-del-gobierno-niega-la-ayuda-a-personas-que-tienen-derecho-a-ella/> accessed 22 July 2024.

[114] Ainhoa, 'EU External Border Control' (*Borderctrl.eu*, 2023) <https://www.iborderctrl.eu/eu-external-border-control.html> accessed 22 July 2024.

automated interview conducted by a virtual border guard assesses whether a person is telling the truth through 16 questions asked by a virtual avatar to be answered and then analysed by a machine.[115] Successively, at the border, facial images, falling within the scope of biometric data as in Art. 4(14) GDPR and captured during the first stage, are compared with the on-site person through live facial recognition and a matching score is calculated. Ultimately, the system generated a single risk score based on a weighted combination of these components.[116] These scoring and non-scoring procedures appear invasive and are believed to be inconsistent with the new AIA. However, it is challenging to classify them under a specific prohibition within this Regulation. The forbidden social scoring practice in the AIA requires an evaluation "*over a certain period of time*",[117] which is not applicable in this case. Art. 5(1)(d) AIA might be relevant, as it prohibits risk assessment that predicts the likelihood of committing a criminal offence based on profiling and/or evaluation of *personality traits*.[118] What is certainly within the scope, though not proscribed but classified as a high-risk AI system, is the use of biometric data for emotion recognition and systems designed to assess the risk of irregular migration, which could be linked to the first phase of the process, i.e. the virtual interview.[119] This classification does not appear to impose limitations on the use of special categories of data, including biometric ones.

From this brief analysis, it is evident that scoring practices are already established or emerging in the EU, extending beyond the well-regulated credit assessment to more personal areas such as social services. However, the question of when a score is provided remains unclear. Legislatively, applying the interpretation from the SCHUFA case, Art. 22 GDPR and its included (even if debatable) safeguards always appear to be relevant. Nonetheless, the forthcoming AIA does not provide clear guidance on these practices, which, as discussed, sometimes appear simultaneously banned and permitted. Apart from

---

[115] Luca Zorloni, 'La Macchina Della Verità Alle Frontiere Dell'Europa è Stata Un Assegno in Bianco' (*Wired*, 2023) <https://www.wired.it/article/iborderctrl-macchina-verita-europa/> accessed 22 July 2024.

[116] 'Automating Society Taking Stock of Automated Decision-Making in the EU' (n 17).

[117] Art. 5(1)(c) AIA.

[118] Art. 5(1)(d) AIA.

[119] Annex III, 1(c); 7(b) AIA.

the aforementioned case related to the specific field of law enforcement, in the other examined examples no use of biometric-based data was identified.

4.2.2 Outside the EU

The second section of this analysis will examine one existing and one potential scoring system implemented outside the European Union, in order to analyse if scoring through biometric or biometric-based data has ever been or will be employed. The discussion will begin with the most well-known and intrusive example, i.e., China's Social Credit System (SCS), followed by a more recent and proximate case in the United Kingdom.

The SCS constitutes a model of data-driven surveillance and societal control.[120] It aims to assess and regulate all facets of citizens' and businesses' activities considered significant by the state, including economic, moral, and political dimensions, across both online and offline spheres.[121] The SCS is designed to evaluate each individual's trustworthiness by utilising a comprehensive national database that aggregates financial and governmental data, ultimately distilling this information into a singular numerical rating for each citizen which leads to tailored rewards (e.g., discounts on utilities or faster internet speeds) and punishments (e.g., job restrictions or blocking purchases of train and plane tickets).[122] The conduct of individuals is managed not through coercion, but by incentivising desirable behaviour and fostering voluntary compliance with state programs and policies. Key sources of information on citizens' behaviour include also prominent Chinese IT companies, such as *Tencent*, which owns the *WeChat* messenger, and *Alibaba*, the biggest Chinese e-commerce platform.[123] Data related to individuals' behaviours are therefore gathered through several platforms which 'feed' the national database. Within

[120] Rogier Creemers, 'China's Social Credit System: An Evolving Practice of Control' [2018] SSRN Electronic Journal <https://www.ssrn.com/abstract=3175792> accessed 22 July 2024.

[121] Anne SY Cheung and Yongxi Chen, 'From Datafication to Data State: Making Sense of China's Social Credit System and Its Implications' (2022) 47 Law & Social Inquiry 1137.

[122] Hans Krause Hansen and Richard Weiskopf, 'From Universalizing Transparency to the Interplay of Transparency Matrices: Critical Insights from the Emerging Social Credit System in China' (2021) 42 Organization Studies 109.

[123] Olga O Bazina, 'Human Rights and Biometric Data. Social Credit System' [2020] Przegląd Europejski 36.

the realm of biometric data, the facial recognition system designated as *Face++* facilitates the generation of meticulous reports on the activities undertaken by individuals outside the electronic network and nourishes the government repository. This functionality is achieved through the tracking of citizens' movements and actions via outdoor video surveillance systems.[124] This instance represents the first documented example of scoring through biometric data identified during the analysis. Unlike the concept of biometric categorisation discussed at the beginning of this Chapter, where individuals are later seen as a group, this case involves analysing specific biometric data of an individual to generate a score, which then determines whether they are allowed or prohibited from engaging in certain activities.

Another example from outside the EU, but in this case within the continent, relates to the United Kingdom. Even if not in force yet, the government is currently developing a digital identity system which could be indirectly used in scoring mechanisms. This framework might encompass income verification for credit scoring and educational qualifications for insurance risk assessments, potentially resulting in greater accuracy in these evaluations.[125] In this case, a broad range of data may be supplied to credit scoring agencies. Although not explicitly stated, it is believed that biometric data could also be collected through the system, e.g. fingerprints, presenting the potential for its use in scoring activities. Unlike China, the UK adopts a data protection approach similar to that of the EU, having incorporated the GDPR and its principles into domestic law. Therefore, it seems complicated to imagine such an invasive procedure to be in line with the legislation in force. However, a comparable analysis cannot be conducted, as there is currently no specific legislation on AI systems in place.

4.3 Do We Have Enough (Clear) Safeguards?

As highlighted in the earlier sections of this Chapter, there appears to be no concrete example of scoring through biometric or biometric-based data in the

[124] ibid.

[125] Matt Warman, 'UK Digital Identity and Attributes Trust Framework Alpha v1 (0.1)' (*GOV.UK*, 2023) <https://www.gov.uk/government/publications/the-uk-digital-identity-and-attributes-trust-framework/the-uk-digital-identity-and-attributes-trust-framework> accessed 27 May 2024.

EU currently in force or planned, excluding the law enforcement sector. However, various initiatives, some more intrusive than others, involving the assessment and evaluation of data subjects are already being implemented within EU Member States. Given the limited case law available for further interpretation, the ambiguity of wording and definitions in the law, as we have seen with the concept of biometric categorisation, as well as potential overlaps of the norms, it is crucial to avoid exceeding acceptable thresholds. Indeed, despite China's geographical and governmental distance, the development of increasingly advanced AI systems could rapidly bridge that gap.

As analysed in the previous Chapter, the GDPR provides only one Article, the 22, which has recently been interpreted to encompass credit scoring activities. The legal basis for such invasive processes appears too easily circumvented or 'collectable'. Specifically, the 'mere' freely given consent of data subjects could allow for the scoring of their biometric data. Furthermore, it is even debatable whether the ECJ's interpretation could apply to other sectors where scoring mechanisms are employed, thus requiring the protection of rights, freedom and legitimate interests, such as human intervention or explication, expressed in the Article. A second issue is the (hidden) existence of 'biometric-based data' that does not fall under Art. 9 GDPR because they do not identify the subject, making it even easier to circumvent protective measures.

The AIA addresses the issue by categorising credit assessment as a high-risk activity and prohibiting social scoring. However, further research has identified various other scoring practices, even if not defined so, in recruitment, social services, and law enforcement. Although future case law will provide interpretation, the current language is believed to be ambiguous regarding whether these different practices are permitted or prohibited. Moreover, as we have seen in this Chapter, the Regulation offers a comprehensive analysis of biometric-based activities, such as biometric categorisation, with most of these processes classified as high-risk rather than prohibited. While the definition of biometric data remains consistent (and arguably too narrow) from the GDPR,[126] it is believed that the delineation of "*personal or personality characteristics*"[127]

[126] Art. 4(14) GDPR.

[127] Art. 5(1)(c) AIA.

is unclear and may potentially encompass a broader category of biometric-based data.

5. Conclusion

Throughout this Master's Thesis, we have examined the regulation and implications of scoring systems within the EU, particularly with regard to biometric data, in the GDPR and the AIA. The initial research question, "*How do the General Data Protection Regulation and the Artificial Intelligence Act regulate scoring systems and protect personal data, specifically biometric and biometric-based ones?*", has been answered through the text. In particular, the investigation began with an analysis of current legal frameworks and their capacity to address the nuances of different data uses, starting with ADM processes. Our research has identified a complex landscape where special categories of data are increasingly being integrated into various sectors, including law enforcement, credit assessment and social services. This implementation has raised significant legal questions, especially concerning the rights of individuals and the potential for misuse.

The GDPR, while providing a robust foundation for data protection, has shown limitations in fully addressing the intricacies of biometric data. Art. 22 GDPR, recently interpreted by the ECJ in the SCHUFA case and which governs ADM, including henceforth (only?) credit scoring, contains provisions that could easily be circumvented due to ambiguities in the definitions and the scope of exceptions allowed. Notably, biometric data – beyond the mere analysis within scoring practices – could escape stringent scrutiny if classified under categories not explicitly covered by Art. 9 GDPR. That is why, a broader concept of biometric-based data has been followed throughout the text.

The AIA introduces a more targeted approach by categorising certain AI applications, including e.g., credit scoring and biometric categorisation, as high-risk activities, while explicitly prohibiting others, such as social scoring. This classification implies a higher level of regulatory oversight and necessitates stringent compliance measures. However, the AIA's language remains somewhat ambiguous, particularly in defining terms like "*personal or personality characteristics"* or *"personality traits"*. This lack of clarity could lead to varying interpretations and potential loopholes that entities might exploit to implement scoring systems infringing upon individual rights.

The examination of concrete examples from within the EU, such as the halted Dutch *Systeem Risico Indicatie* (SyRI), underscores the social

implications of scoring practices. This example has highlighted the tension between technological advancement and legal safeguards, illustrating the need for clear, enforceable regulations that can adapt to rapid technological changes.

Furthermore, the comparison with practices outside the EU, such as the SCS in China, intrusive instance of social scoring, provided a broader perspective on the global regulatory environment. China's extensive use of special categories of data, including biometric information, in this type of scoring starkly contrasts with EU principles. While these practices may seem physically and mentally distant from those employed within the EU, their potential misuse still necessitates robust preventive measures.

This Master's Thesis has tried to underscore the lack of a comprehensive and clear regulatory framework for scoring systems, especially for the possible future employment of special categories of data, such as biometric ones. The definition of biometric data present in the GDPR, as referenced in the AIA, has been found to be overly narrow. While both Regulations have laid foundational principles and categorisation efforts, they require further refinement and clarification to effectively protect fundamental rights in the face of advancing AI technologies. Future case law will play a crucial role in interpreting these norms and ensuring they adapt to emerging challenges. For instance, national courts may request preliminary rulings from the CJEU to clarify ambiguities and inconsistencies within the legislative texts. Strategic litigation could also be employed to provoke judicial interpretation and set precedents that better align with the protection of fundamental rights.

The balance between innovation and protection of rights, such as privacy and dignity, must be properly scaled, ensuring that neither side tips too far.

List of References

1. Legal Sources

1.1 Legislative and Other Legal Acts

1.1.1 European

Charter of Fundamental Rights of the European Union [2012] OJ C 326/391

Consolidated Version of the Treaty on the Functioning of the European Union [2012] OJ C 326/47

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 L 119/1

Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act) [2024] OJ L 9/144

1.1.2 National

Art. 117 of the (Italian) Code in Legislative Decree No. 196/2003

Paragraph 31 of the Bundesdatenschutzgesetz (German Federal Law on data protection) of 30 June 2017 (BGBI. I, p. 2097; 'the BDSG'), 'Protection of trade and commerce in the context of "scoring" and credit reports'

1.2 Case Law

1.2.1 European

Case C-252/21 *Meta Platforms and Others* [2023] ECLI:EU:C:2023:537

Case C-634/21 *SCHUFA Holding (Scoring)* [2023] ECLI:EU:C:2023:957

1.2.2 National

Rechtbank Den Haag, ECLI:NL:RBDHA:2020:1878 [2020] (The Netherlands)

1.3 Other Legal or Policy Documents

'Automating Society Taking Stock of Automated Decision-Making in the EU' (AlgorithmWatch 2019) <https://algorithmwatch.org/en/wp-content/uploads/2019/02/Automating_Society_Report_2019.pdf>

Article 29 Data Protection Working Party, 'Opinion 3/2012 on developments in biometric technologies' (2012) <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2012/wp193_en.pdf>

Article 29 Data Protection Working Party, 'Guidelines on automated individual decision-making and profiling for the purposes of regulation 2016/679' (2018) <https://ec.europa.eu/newsroom/article29/items/612053/en>
Backer L C, 'Measurement, Assessment and Reward: The Challenges of Building Institutionalized Social Credit and Rating Systems in China and in the West' [2017] Conference: The Chinese Social Credit System 2017

Case C-634/21 *SCHUFA Holding (Scoring)* [2023], Opinion of AG Pikamaë ECLI:EU:C:2023:220

Council of Europe, 'Explanatory Report to the Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data' (2018) <https://rm.coe.int/cets-223-explanatory-report-to-the-protocol-amending-the-convention-fo/16808ac91a>

Dencik L, Hintz A, Redden J, and Warne H, 'Data Scores as Governance: Investigating Uses of Citizen Scoring in Public Services. Project Report' [2018] Data Justice Lab Cardiff University 10

European Data Protection Board, 'Guidelines 3/2019 on Processing of Personal Data through Video Devices' (2020) <https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201903_video_devices_en_0.pdf>

European Data Protection Board, 'Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement' (2023) <https://www.edpb.europa.eu/system/files/2023-05/edpb_guidelines_202304_frtlawenforcement_v2_en.pdf>

European Parliament, Directorate General for Internal Policies., *Biometric Recognition and Behavioural Detection.* (Publications Office 2021) <https://www.europarl.europa.eu/RegData/etudes/STUD/2021/696968/IPOL_STU(2021)696968_EN.pdf>

High-level Expert Group on Artificial Intelligence, 'Ethics Guidelines for Trustworthy AI' (2019) <https://www.aepd.es/sites/default/files/2019-09/ai-definition.pdf>

Loefflad C and Grossklags J, 'How the Types of Consequences in Social Scoring Systems Shape People's Perceptions and Behavioral Reactions', *The 2024 ACM Conference on Fairness, Accountability, and Transparency* (ACM 2024) <https://dl.acm.org/doi/10.1145/3630106.3658986>

Pearson A, 'How to Use AI and Personal Data Appropriately and Lawfully' (Information Commissioner's Office (UK) 2022) <https://policycommons.net/artifacts/3534587/how-to-use-ai-and-personal-data-appropriately-and-lawfully/4335800/>

Spanish Data Protection Authority, 'Use of Biometric Data: Assessment from a Data Protection Perspective' (*AEPD*, 2022) <https://www.aepd.es/en/prensa-y-comunicacion/blog/biometric-data-assessment-from-a-data-protection-perspective>

UNESCO, 'Recommendation on the Ethics of Artificial Intelligence' [2021] <https://unesdoc.unesco.org/ark:/48223/pf0000381137>

Warman M, 'UK Digital Identity and Attributes Trust Framework Alpha v1 (0.1)' (*GOV.UK*, 2023) <https://www.gov.uk/government/publications/the-uk-digital-identity-and-attributes-trust-framework/the-uk-digital-identity-and-attributes-trust-framework>

2. Academic Sources

2.1 Books

Matejka J, Krausová A and Güttler V, *Biometric Data and Its Specific Legal Protection* (Institute of State and Law of the Czech Academy of Sciences 2020)

Mayer-Schönberger V and Cukier K, *Big Data: A Revolution That Will Transform How We Live, Work and Think* (1. publ, Murray 2013)

2.2 Book Chapters

Bygrave L A, 'Article 22 Automated Individual Decision-Making, Including Profiling' in Christopher Kuner and others (eds), *The EU General Data Protection Regulation (GDPR)* (Oxford University PressNew York 2020)

Granmar C G, 'AI-Based Decision-Making and the Human Oversight Requirement Under the AI Act' in Eduardo Gill-Pedro and Andreas Moberg (eds), *YSEC Yearbook of Socio-Economic Constitutions 2023*, vol 2023 (Springer Nature Switzerland 2024)

Langenbucher K and Corcoran P, 'Responsible AI Credit Scoring – A Lesson from Upstart.Com' in Emilios Avgouleas and Heikki Marjosola (eds), *Digital Finance in Europe: Law, Regulation, and Governance* (De Gruyter 2021)

Mendoza I and Bygrave L A, 'The Right Not to Be Subject to Automated Decisions Based on Profiling' in Tatiana-Eleni Synodinou and others (eds), *EU Internet Law* (Springer International Publishing 2017)

Rieder G and Simon J, 'Big Data: A New Empiricism and its Epistemic and Socio-Political Consequences' in Wolfgang Pietsch, Jörg Wernecke and Maximilian Ott (eds), *Berechenbarkeit der Welt?* (Springer Fachmedien Wiesbaden 2017)

Silveira A, 'Profiling and Cybersecurity: A Perspective from Fundamental Rights' Protection in the EU' in Francisco António Carneiro Pacheco De Andrade, Pedro Miguel Fernandes Freitas and Joana Rita De Sousa Covelo De Abreu (eds), *Legal*

Developments on Cybersecurity and Related Fields, vol 60 (Springer International Publishing 2024)

2.3 Journal Articles

Aizenberg E and Van Den Hoven J, 'Designing for Human Rights in AI' (2020) 7 Big Data & Society 205395172094956

Appelman N, Ó Fathaigh R, and van Hoboken J, 'Social Welfare, Risk Profiling and Fundamental Rights: The Case of SyRI in the Netherlands' [2021] JIPITEC 257

Bazina O O, 'Human Rights and Biometric Data. Social Credit System' [2020] Przegląd Europejski 36

Cheung A SY and Chen Y, 'From Datafication to Data State: Making Sense of China's Social Credit System and Its Implications' (2022) 47 Law & Social Inquiry 1137

Creemers R, 'China's Social Credit System: An Evolving Practice of Control' [2018] SSRN Electronic Journal

Davis P and Schwemer S F, 'Rethinking Decisions Under Article 22 of the GDPR: Implications for Semi-Automated Legal Decision-Making' [2023] SSRN Electronic Journal

De Cooman J, 'Humpty Dumpty and High-Risk AI Systems: The Ratione Materiae Dimension of the Proposal for an EU Artificial Intelligence Act' [2022] Market and Competition Law Review 49

Dencik L and others, 'The "Golden View": Data-Driven Governance in the Scoring Society' (2019) 8 Internet Policy Review

Dreyer S, Schulz W and Stiftung B, 'The General Data Protection Regulation and Automated Decision-Making: Will It Deliver?: Potentials and Limitations in Ensuring the Rights and Freedoms of Individuals, Groups and Society as a Whole' [2019] Discussion paper Ethics of Algorithms

Ebers M, 'Chapter 2: Regulating AI and Robotics: Ethical and Legal Challenges' [2019] SSRN Electronic Journal

Ebers M and others, 'The European Commission's Proposal for an Artificial Intelligence Act—A Critical Assessment by Members of the Robotics and AI Law Society (RAILS)' (2021) 4 J 589

Faivre J, 'The AI Act: Towards Global Effects?' [2023] SSRN Electronic Journal

Fanni S, 'The Biometric Habeas Data in the Digital and Algorithmic Era in the European Union' (2023) 3 Latin American Journal of European Studies 18

Falletti E, 'Credit Scoring Under Scrutiny by the Court of Justice of the European Union: Brief Remarks on the "SCHUFA Decision"' [2024] SSRN Electronic Journal

Ferrer X and others, 'Bias and Discrimination in AI: A Cross-Disciplinary Perspective' (2021) 40 IEEE Technology and Society Magazine 72

Hupont I and others, 'The Landscape of Facial Processing Applications in the Context of the European AI Act and the Development of Trustworthy Systems' (2022) 12 Scientific Reports 10688.

Jia L, 'Unpacking China's Social Credit System: Informatization, Regulatory Framework, and Market Dynamics' (2020) 45 Canadian Journal of Communication 113

Keats Citron D and Pasquale F, 'The Scored Society: Due Process for Automated Predictions' (2014) 89 Washington Law Review

Krause Hansen H and Weiskopf R, 'From Universalizing Transparency to the Interplay of Transparency Matrices: Critical Insights from the Emerging Social Credit System in China' (2021) 42 Organization Studies 109

Langenbucher K, 'Responsible A.I.-Based Credit Scoring – A Legal Framework' (2020) 31 European Business Law Review 527

Langer P F, 'Lessons from China - The Formation of a Social Credit System: Profiling, Reputation Scoring, Social Engineering', *The 21st Annual International Conference on Digital Government Research* (ACM 2020) <https://dl.acm.org/doi/10.1145/3396956.3396962>

Mann M and Matzner T, 'Challenging Algorithmic Profiling: The Limits of Data Protection and Anti-Discrimination in Responding to Emergent Discrimination' (2019) 6 Big Data & Society 205395171989580

McLean S and others, 'The Risks Associated with Artificial General Intelligence: A Systematic Review' (2023) 35 Journal of Experimental & Theoretical Artificial Intelligence 649

Meszaros J, Minari J, and Huys I, 'The Future Regulation of Artificial Intelligence Systems in Healthcare Services and Medical Research in the European Union' (2022) 13 Frontiers in Genetics 927721

Natgunanathan I and others, 'Protection of Privacy in Biometric Data' (2016) 4 IEEE Access 880

Paal B, 'Case Note: Article 22 GDPR: Credit Scoring Before the CJEU' (2023) 4 Global Privacy Law Review 127

Pagan N and others, 'A Classification of Feedback Loops and Their Relation to Biases in Automated Decision-Making Systems', *Equity and Access in Algorithms, Mechanisms, and Optimization* (ACM 2023)

Schuett J, 'Risk Management in the Artificial Intelligence Act' [2023] European Journal of Risk Regulation 1

Silveira A, 'Automated Individual Decision-Making and Profiling [on Case C-634/21 - SCHUFA (Scoring)]' (2023) 8 UNIO – EU Law Journal 74

Wang J, Li H and Xu W, 'Envisioning a Credit Society: Social Credit Systems and the Institutionalization of Moral Standards in China' (2023) 45 Media, Culture & Society 451

Yang C S and Dobbie W, 'EQUAL PROTECTION UNDER ALGORITHMS: A NEW STATISTICAL AND LEGAL FRAMEWORK' (2020) 119 Michigan Law Review 291

Zuiderveen Borgesius F and Poort J, 'Online Price Discrimination and EU Data Privacy Law' (2017) 40 Journal of Consumer Policy 347

3. Non-Academic Sources

'Candidate Scoring' (*HiPeople*, 2023) <https://www.hipeople.io/glossary/candidate-scoring>

'EU: Artificial Intelligence Regulation Should Ban Social Scoring' (*Human Rights Watch*, 2023) <https://www.hrw.org/news/2023/10/09/eu-artificial-intelligence-regulation-should-ban-social-scoring>

'The Opportunity For AI In Vendor Management Systems' (*Simplify beyond the vms*, 2021) <https://www.simplifyvms.com/resources/blogs/ai-in-recruitment/the-opportunity-for-ai-in-vendor-management-systems/>

'The Siry Case Netherlands, Court of the Hague: Systeem Risico Indicatie (SyRI)' (*AI Taxadmin.EU*) <https://www.uantwerpen.be/en/projects/aitax/publications/syri/>

Ainhoa, 'EU External Border Control' (*Borderctrl.eu*, 2023) <https://www.iborderctrl.eu/eu-external-border-control.html>

Belmonte E, 'La Aplicación Del Bono Social Del Gobierno Niega La Ayuda a Personas Que Tienen Derecho a Ella' (*CIVIO*, 2019) <https://civio.es/tu-derecho-a-saber/2019/05/16/la-aplicacion-del-bono-social-del-gobierno-niega-la-ayuda-a-personas-que-tienen-derecho-a-ella/>

Garante per la Protezione dei Dati Personali, '"Cittadinanza a punti": Garante privacy ha avviato tre istruttorie. Preoccupanti i meccanismi di scoring che premiano i cittadini "virtuosi"' [2022] <

https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9778361>

Gyevnar B, Ferguson N and Schafer B, 'Bridging the Transparency Gap: What Can Explainable AI Learn From the AI Act?' <https://arxiv.org/abs/2302.10766>

Kayser-Bril N, 'Personal Scoring in the EU: Not Quite Black Mirror yet, at Least If You're Rich' (*Algorithm Watch*) <https://algorithmwatch.org/en/personal-scoring-in-the-eu-not-quite-black-mirror-yet-at-least-if-youre-rich/>

Lawrence-Archer A and Naik R, 'Effective Protection against AI Harm' (AWO Agency 2023) <https://www.awo.agency/blog/awo-analysis-shows-gaps-in-effective-protection-from-ai-harms/>

Pucarelli F and Collini M, 'Intelligenza Artificiale e Protezione Dei Dati: Una Convivenza Possibile?' (*Stefanelli&Stefanelli*, 2023) <https://www.studiolegalestefanelli.it/it/approfondimenti/intelligenza-artificiale-e-protezione-dei-dati-una-convivenza-possibile/>

Quantumrun Foresight, 'Biometric scoring: Behavioral biometrics might verify identities more accurately' [2023] < https://www.quantumrun.com/insight/biometric-scoring-behavioral-biometrics-might-verify-identities-more-accurately>

Zorloni L, 'La Macchina Della Verità Alle Frontiere Dell'Europa è Stata Un Assegno in Bianco' (*Wired*, 2023) <https://www.wired.it/article/iborderctrl-macchina-verita-europa/>