Credit scoring judicial review between the Court of Justice of the European Union and comparative case law*

Elena Falletti, Chiara Gallese

Abstract

Credit scoring is a widespread practice that assigns a score based on certain characteristics or past behaviors, in particular regarding the reliability of debtors to repay loans. In this regard, the new Regulation on Artificial Intelligence (AI Act) adds a control tool to the already well-known art. 22 GDPR, in order to protect consumers and weaker parties, based on which the Court of Justice of the European Union issued the *SCHUFA* decision. However, there are still grey areas in which the balance between the transparency owed to the consumers regarding the processing of their data or the protection of trade secrets in favor of credit score agencies.
This article analyses the orientations of the Court of Justice of the European Union and the national courts regarding credit scoring, following the *SCHUFA* decision, and proposes some reflections on the application of arts. 22 GDPR and 86 AI Act in this context.

Il credit scoring è una pratica diffusa che assegna un punteggio sulla base di alcune caratteristiche o comportamenti passati, in particolare in merito all'affidabilità dei debitori di rimborsare i prestiti ricevuti. A questo proposito, il nuovo regolamento sull'Intelligenza Artificiale (AI Act) aggiunge uno strumento di controllo al già noto art. 22 del GDPR per tutelare i consumatori e le parti deboli, sulla base del quale la Corte di giustizia dell'Unione europea ha emesso la decisione SCHUFA. Tuttavia, esistono ancora aree grigie in cui il bilanciamento tra la trasparenza dovuta ai consumatori in merito al trattamento dei loro dati e la protezione dei segreti commerciali è a favore delle agenzie di credit score.
Questo articolo analizza gli orientamenti della Corte di giustizia dell'Unione europea

*Author contribution: the abstracts and section 1 were written by both authors; Elena Falletti wrote sections 2, 3, and 6; Chiara Gallese wrote sections 4, 5 and 7. This work was partially funded by the European Union, DataCom Project, Grant Agreement no. 101108151. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or European Commission and EU executive agencies.
Neither the European Union nor the granting authority can be held responsible for them.
L'articolo è stato sottoposto, in conformità al regolamento della Rivista, a referaggio "a doppio cieco".

e dei tribunali nazionali in materia di credit scoring a seguito della decisione SCHUFA e propone alcune riflessioni sull'applicazione degli artt. 22 del GDPR e 86 dell'AI Act in questo contesto.

Table of contents

1. Introduction. – 2. The *SCHUFA* decision by the Court of Justice of the European Union. - 3. Advocate General De La Tour's conclusions in the CK case on the relationship between access to information and protection of trade secrets. – 4. The right to technical interpretability and AI automated decision-making - 5. Is a remedial coexistence between art. 22 GDPR and art. 86 AI Act possible? - 6. The comparative case-law following the *SCHUFA* ruling. - 7. Conclusions

Keywords

Artificial Intelligence – Automated Decision Making – Credit Scoring – Transparency – Comparative Law

1. Introduction

Credit scoring is a statistical method used by banks, other financial institutions, and international agencies to assess the creditworthiness of individuals or businesses applying for credit. Those actors evaluate several financial and non-financial factors to determine the likelihood that a borrower will repay their debt obligations on time. Credit rating agencies played a crucial role in the 2007-2008 crisis by assigning overly optimistic ratings to complex financial instruments, such as subprime mortgages[1]. These inflated ratings gave investors a false sense of security, leading to excessive risk-taking and ultimately contributing to the collapse of the housing bubble and the worldwide crisis[2].

However, such tools can have several negative effects on individuals, that are particularly pronounced for certain demographic groups[3], and can have long-lasting consequences on financial well-being. For example, Consumers who experience a credit rating downgrade, even due to factors beyond their control, may face reduced access to financing for extended periods[4].

Automation and algorithm-driven decision-making systems have transformed the consumer finance industry. What once relied heavily on human judgment has increas-

[1] Z. Guo, *The 2008 Financial Crisis: Causes, Consequences, and Responses* in *Highlights in Business,* in *Economics and Management*, 27, 2024, 373 ss.; A. Astakhova-S Grishunin-G. Pomortsev, *Developing a Scoring Credit Model Based on the Methodology ofInternational Credit Rating Agencies,* in *Journal of Corporate Finance Research*, 2023, 17(1), ss., doi.org/10.17323/j.jcfr.2073-0438.17.1.2023.5-16.

[2] *Ibidem.*

[3] L. Blattner-S. Nelson, *How costly is noise? Data and disparities in consumer credit*, in *arXiv preprint,* arXiv:2105.07554, 2021.

[4] J. M. Garmaise-G. Natividad, *Slippery Slope or Wake-up Call? Negative Credit Rating Shocks for Consumers*, in UCLA Working Paper, 2016.

ingly been shifted to data-driven processes, fueled by large amounts of personal and financial data ("big data"). The rise of AI credit scoring systems, and more recently, "credit analytics" has increased in recent years. However, while automation promises efficiency and objectivity, it often introduces new forms of opacity and discrimination that are largely invisible and hard to challenge. As noted by Pasquale[5], it is not uncommon for consumers to learn that their poor credit score has cost them tens of thousands of dollars over the course of a mortgage or other long-term loans. Yet, how these scores are calculated remains largely a mystery, hidden behind proprietary algorithms and trade secrets that are not open to public scrutiny[6]. While there are general guidelines on what factors influence a credit score (such as payment history, amounts owed, and length of credit history) the precise formula is unknown[7]. This secrecy causes consumers several troubles, as they are unable to fully understand the basis on which their financial credibility is judged[8].

Furthermore, there is the additional problem of relevance, accuracy, and timeliness of data, which are all indicators of data quality. As known, the quality of data influences the results of any analysis, whether it is based on AI or not, as it is impossible to produce an accurate output from inaccurate data. Therefore, data subjects who are the object of such analysis have a strong interest in credit-scoring players keeping their data as accurate as possible to avoid unfair decisions.

However, due to the opacity of these systems, it is impossible to know how, when, and how often credit-scoring agencies update personal data in their databases. Without proper transparency measures, it is very difficult for data subjects to exercise their right to correct their data according to GDPR, as in order to do so it is necessary to know that an error exists in the first place. For example, it is often the case that consumer discovers after many months or even years that their name has been wrongly connected to insolvency cases due to identity theft, and this causes a significant amount of trouble, starting from the impossibility of accessing credit.

If the prison for debt no longer has metal bars as it did for Little Dorrit and her family[9], the (bad) reputation of debt still has significant consequences that can bog down the existential path of the debtor and by extension, of his family imprisoned by more intangible, but no less effective constraints such as databases of "bad payers"[10] and credit scoring algorithms[11].

[5] F. Pasquale, *The Credit Scoring Conundrum*, in *U of Maryland Legal Studies Research Paper,* 2013, 2013-45.

[6] *Ibidem*.

[7] *Ibidem*.

[8] *Ibidem*.

[9] C. Dickens, *Little Dorrit, Povertry,* London, 1857.

[10] R. Muñoz-Cancino-C. Bravo–S. A. Ríos–M. Graña, *On the dynamics of credit history and social interaction features, and their impact on creditworthiness assessment performance,* in *Expert Systems with Applications,* 2023, 2018, 119599; M. S. Moghe–S. Johri, *The Role of Credit Scoring in Modern Banking–An Overview of Methodology & Implementation*, in *UNNAYAN*, XVI, 2024, 209 ss.

[11] X. Zhang - L.Yu. *Consumer credit risk assessment: A review from the state-of-the-art classification algorithms, data traits, and learning methods*, in *Expert Systems with Applications* 237, 2024, 121484; A. Bhattacharya, - S. K. Biswas, - A. Mandal, *Credit risk evaluation: a comprehensive study*, in *Multimedia Tools and Applications* 82, 12, 2023, 18217 ss.

What seems objectionable about such systems is that they collect data on both significant defaults (e.g., mortgage payments) and smaller defaults (e.g., missed bill payments), as well as information on personal lifestyles through web scraping of information posted online[12].

From one's "onlife"[13]", an endless multitude of information emerges, forming "fingerprints"[14], that can be used by credit scoring algorithms to better focus both the creditworthiness and the lifestyle and even the personality of the person who is getting into debt.

Credit scoring programs are a subset of predictive software that falls under the umbrella of social scoring[15]. These programs, which generally assess financial reliability, are part of a category of software that evaluates individuals' adherence to socially acceptable behaviors within a community[16].

Social scoring aims to measure an individual's reliability in all aspects, integrating whatever data can be collected on a subject into the calculation[17]. Applying such a concept to the possible predictability of repayment of the loan or mortgage obtained, it is a score developed through a statistical procedure. This procedure quantifies the probability of a person's future solvency based on a combination of the payments made in the past by the same person and their classification within a category of similar subjects, according to their individual characteristics[18].

It's important to note that the starting point for machine learning in credit scoring combines past factors and the social category to which the individual belongs, deduced from their personal characteristics. These characteristics play a meaningful role in the social scoring process. This individual may wish to exercise the fundamental right to be forgotten[19], especially in a sensitive area like insolvency. On this point, the

[12] L. Crosato-J. Domenech–C. Liberati, *Websites' data: a new asset for enhancing credit risk modeling*, in *Annals of Operations Research*, 342, 2024, 1671 ss.

[13] L. Gambacorta-Y. Huang-H. Qiu-J.I Wang, *How do machine learning and non-traditional data affect credit scoring? New evidence from a Chinese fintech firm*, in *Journal of Financial Stability*, 73, 2024, 101284.

[14] L. Floridi, *The Onlife Manifesto Being Human in a Hyperconnected Era*, Cham, 2015, *passim*.

[15] C. Loefflad-J. Grossklags, *How the Types of Consequences in Social Scoring Systems Shape People's Perceptions and Behavioral Reactions*, in *The 2024 ACM Conference on Fairness, Accountability, and Transparency*, 2024, 1515-1530; K. Crawford, *Atlas of AI*, New Haven – London, 2021, 205 ss.

[16] W. Rabe-G. Kostka, *Perceptions of social credit systems in Southeast Asia: An external technology acceptance model,* in *Global Policy*, 2024; G. Cerrina Feroni, *Intelligenza artificiale e sistemi di "scoring" sociale. Tra distopia e realtà*, in *Diritto dell'informazione e dell'informatica*, 1, 2023, 1 ss.

[17] G. Gigerenzer, *Perché l'intelligenza umana batte ancora gli algoritmi*, Milano, 2023, 201.

[18] M. Pincovsky-A. Falcão-W. N. Nunes-A. Paula Furtado-R. C. L. V. Cunha, *Machine Learning applied to credit analysis: a Systematic Literature Review,* in *2021 16th Iberian Conference on Information Systems and Technologies (CISTI)*, Chaves, Portugal, 2021, 1-5, doi: 10.23919/CISTI52073.2021.9476350; M. Bücker, et al., *Transparency, auditability, and explainability of machine learning models in credit scoring*, in *Journal of the Operational Research Society* 73.1, 2022, 70 ss.

[19] CJEU, C-131/12, *Google Spain SL and Google Inc. v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González* (2014). See A. Palmieri-R. Pardolesi, *Diritto all'oblio: il futuro dietro le spalle*, in *Il Foro Italiano*, 6, 2014, 317 ss; C. Wolf, *Impact of the CJEU's Right to Be Forgotten: Decision on Search Engines and other Service Providers in Europe: Case C-131/12 Google v. Agencia Española de Protetción de Datos (AEPO) and Mario Costeja Gonzalez, Judgment of 13 May 2014*, in *Maastricht Journal of European and Comparative Law,* 3, 2014, 547 ss.; S. Shuntich, *The Life, the Death, and the long-Awaited Resurrection of Privacy* in *Human Rights*, 4, 2014, 2.

debtor needs to be aware of what information referable to him is used in the profiling programs and thus have access to meaningful information on both the authenticity of the data and the logic used in the credit scoring process.

The credit scoring software formalizes an evaluation that, unfortunately, is not free from potential group or classist bias[20], based on one's (potentially outdated) reputation.

This article is developed as follows: first, the litigation that has taken place and is pending before the Court of Justice is analysed, then the remedies that can be used against automated decisions, i.e., art. 22 GDPR and art. 68 AI Act, are compared, then the precedents after the *SCHUFA* decision are discussed, and finally some summary conclusions are outlined.

2. The *SCHUFA* decision by the Court of Justice of the European Union

SCHUFA (Schutzgemeinschaft für allgemeine Kreditsicherung) is a private German company that plays a crucial role in the country's credit reporting and financial services sector. Its primary purpose is to collect, store, and provide information about individuals' and businesses' creditworthiness. This information helps banks, businesses, and other entities make informed decisions about lending money, extending credit, or entering into contracts[21].

The *SCHUFA* case involves an individual who was denied a loan based on a negative credit score provided by SCHUFA to their financial institution. The applicant, suspecting inaccuracies, approached SCHUFA to request information regarding the data stored about them and to challenge the accuracy of their credit score. They also demanded a detailed explanation of how SCHUFA calculated their credit score, as well as the significance and possible consequences of such processing, citing art. 15(1)(h) of the General Data Protection Regulation (GDPR). However, SCHUFA responded by giving the applicant only the credit score and a vague description of its calculation methodology, but not on what specific information was included in the mathematical operation and how it was weighted, arguing that providing a detailed explanation of the scoring process was not possible since it would infringe on its commercial secrecy[22]. SCHUFA also claimed that its obligations under the GDPR were limited because it only provided information to third parties, like banks, and did not make the final decisions directly, such as approving or denying loans.

[20] O. B. Deho-L. Liu-J. Li-J. Liu-C. Zhan-S. Joksimovic, *When the past!= the future: Assessing the Impact of Dataset Drift on the Fairness of Learning Analytics Models*, in *IEEE Transactions on Learning Technologies,* 2024; A. Castelnuovo et al., *Befair: Addressing fairness in the banking sector*, in *2020 IEEE International Conference on Big Data (Big Data)*, IEEE, 2020, 3653; S. Verma-J. Rubin, *Fairness definition explained*, in *2018 IEEE/ACM International Workshop on Software Fairness (FairWare)*, IEEE, 2018, 1 ss.

[21] A. Asymina, *Scores as Decisions? Article 22 GDPR and the Judgment of the CJEU in SCHUFA Holding (Scoring)* in the *Labour Context, Industrial Law Journal*, 2024, dwae035, /doi.org/10.1093/indlaw/dwae035.

[22] This is a matter of litigation pending before the Court of Justice, which will be dealt with in the next paragraph.

This case brings into focus key questions about transparency in automated decision-making under the GDPR, particularly how much information credit scoring agencies like SCHUFA must disclose about their algorithms. It also touches on the balance between individuals' rights to understand how their personal data is processed and companies' rights to protect trade secrets.

After the refusal, the client escalated their complaint against SCHUFA to the Hessian Commissioner for Data Protection and Freedom of Information (HBDI), i.e. the German national data protection authority. The applicant requested the HBDI to compel SCHUFA to reveal the specific logic behind their credit score calculation, as well as the significance and potential consequences of the data processing, invoking their rights under the GDPR. However, the HBDI declined to take action against SCHUFA for two years, eventually dismissing the complaint. The authority justified the credit scoring company as complying with Section 31 of the Federal Data Protection Act (BDSG)[23], requirements, which contains detailed rules on scoring procedure and creditworthiness information.

The client contested this ruling before the Amtsgericht Wiesbaden, the ordinary court, which then sought clarification from the Court of Justice of the European Union. The referring court was grappling with the question of whether art. 22(1) GDPR applied to the automated procedure for determining the probability of default rate. This was a crucial issue, as art. 22(1) of GDPR is designed to protect (natural) persons from the discriminatory risks of purely automated decisions. The main question was whether SCHUFA's credit score, which was essentially a probability value derived from profiling, could be considered an automated decision that significantly impacts individuals when relied upon by a third party, like a bank, to make decisions about

[23] §31 BDSG entitled: "*Schutz des Wirtschaftsverkehrs bei Scoring und Bonitätsauskünften*". In addition to the controversy that occurred before the VG Wiesbaden, there is extensive case law applying this rule in the German legal system. Among the most significant rulings are (source: *dejure.org*): LG Frankfurt/Main, 26/05/2023 - 24 O 156/21 concerning the illegal reporting of electricity supply contract customers to SCHUFA; LG Mainz, 12/11/2021 - 3 O 12/20, regarding liability for illegal reporting; OLG Naumburg, 10/03/2021 - 5 U 182/20, on credit card contractual conditions; LG Frankenthal, 28/06/2022 - 8 O 163/22, for reporting to SCHUFA despite a dispute; VG Wiesbaden, 27/09/2021 - 6 K 549/21, on the right to erasure for illegal reporting to SCHUFA; KG (Kammergericht), 30/07/2019 - 4 U 90/19 on the revocation of negative registrations made with SCHUFA; LG Lüneburg, 14/07/2020 - 9 O 145/19 on the legitimacy of the interest in data transmission for a small current account overdraft; LG Hannover, 14/02/2022 - 13 O 129/21, on compensation for unauthorized reporting to SCHUFA; OLG Brandenburg, 03/07/2023 - 1 U 8/22, cited on the adequacy of the data retention period (3 years) by the credit agency; OLG Koblenz, 18/05/2022 - 5 U 2141/21 and LG Bonn, 23/10/2019 - 1 O 322/19, both concerning requests for data related to a mobile phone contract; LG München I, 25/04/2023 - 33 O 5976/22, on the transmission of personal data by a telephone company to SCHUFA; OLG Düsseldorf, 11/01/2022 - 16 U 130/21, on asserting the right to informational self-determination in the credit sector; LG Karlsruhe, 02/08/2019 - 8 O 26/19, denial of the applicability of art. 82 GDPR following the processing of a negative score by SCHUFA; OLG Frankfurt, 15/03/2023 - 17 U 134/22, liability for incorrect registration with SCHUFA; LG Arnsberg, 16/06/2020 - 1 O 44/20 on SCHUFA's duty to delete negative information; VG Wiesbaden, 07/06/2021 - 6 K 307/20, regarding the registration of debtors' negative data; LG Osnabrück, 29/04/2020 - 18 O 400/19, concerning insolvency threats; OLG Schleswig, 03/06/2022 - 17 U 5/22, on the registration of a planned insolvency procedure, VG Wiesbaden, 24/09/2021 - 6 K 442/21, on the legitimacy of the supervisory authority's intervention; LG Hamburg, 23/07/2020 - 334 O 161/19, on the conditions for the existence of the right to data erasure after debt extinction; OLG Koblenz, 25/03/2020 - 12 U 2228/19, on the right of rectification of the debtor served with an injunction.

loans or other contracts. The main query was at which stage of the creditworthiness assessment the automated calculation procedure came into play: (a) at the assessment stage, based on data provided by third parties (e.g., the bank) to SCHUFA; (b) in the actual calculation phase.

The CJEU was asked to determine if the mere issuance of a credit score (probability value) by SCHUFA qualifies as such a decision, given that a third party (like a bank) relies on it in making an official, impactful decision—such as denying a loan, which has clear legal and financial consequences. The core legal question is whether the credit score itself, issued by SCHUFA in the first place, can be considered a "decision" under art. 22(1) of the GDPR. Art. 22(1) provides that individuals have the right not to be subject to decisions based solely on automated processing, including profiling, if those decisions produce legal effects or similarly significant impacts on them.

The CJUE first stated that the application of art. 22 GDPR must consider both the wording and the context, objectives, and purposes that an automated decision pursues[24], as well as the fact that the decision does not contain human intervention[25]. Three conditions must coexist for the applicability of art. 22, namely: a) that a decision is necessary[26]; b) that it must be «based solely on automated processing, including profiling», and c) that it must produce «legal effects [concerning the data subject]» or affect «his or her person in a similarly significant way».

As regards point (a), the definition provided in recital 71, according to which, in order to be such, a decision must involve the assessment of the personal aspects of a data subject, who has a right to opt out of that decision if it «significantly» affects their person. In other words, the data subject is entitled to evade the legal effects produced by a purely automated decision affecting them, as in the case of the automated rejection of an online credit application or online recruiting practices managed by algorithms[27].

[24] CJEU, C-579/21, *Pankki* S. (2023), EU:C:2023:501, § 38.

[25] P. Hacker–J. Cordes–J. Rochon, *Regulating Gatekeeper Artificial Intelligence and Data: Transparency, Access and Fairness under the Digital Markets Act, the General Data Protection Regulation and Beyond* in *European Journal of Risk Regulation* 15, 1, 2024, 49 ss.

[26] Under this point, the Advocate General Pikamäe affirmed that «On these points, the Court of Justice aligns with the conclusions of the Advocate General, according to whom "(T)he absence of a legal definition (of decision) indicates that the EU legislature opted for a broad concept which can include a number of acts capable of affecting the data subject in many ways". In this sense, «a "decision" within the meaning of Article 22(1) of the GDPR can either have "legal effects" or "similarly" affect the data subject, which means that the "decision" in question may have an impact that is not necessarily legal but rather economic and social. Since Article 22(1) of the GDPR seeks to protect natural persons against the potentially discriminatory and unfair effects of automated processing of data, it seems that particular vigilance is required and must also be reflected in the interpretation of that provision» (Opinion of the Advocate General Pikamäe, Case C-634/21, 16 March 2023).

[27] S. Ochmann et al., *Perceived algorithmic fairness: An empirical study of transparency and anthropomorphism in algorithmic recruiting*, in *Information Systems Journal,* 34, 2024, 384 ss.; D. Narayanan-M. Mahak–McGuire–S. Schweitzer-D. De Cremer, *Fairness perceptions of artificial intelligence: A review and path forward,* in *International Journal of Human–Computer Interaction* 40, 2024, 4 ss. Recital 71 reads: «The data subject should have the right not to be subject to a decision, which may include a measure, evaluating personal aspects relating to him or her which is based solely on automated processing and which produces legal effects concerning him or her or similarly significantly affects him or her, such as automatic refusal of an online credit application or e-recruiting practices without any human intervention. Such processing includes "profiling" that consists of any form of automated processing of personal data evaluating the personal aspects relating to a natural person, in particular to analyse or predict aspects concerning

The decision referenced aligns with art. 22(1) of GDPR applied to credit scoring activities like those conducted by SCHUFA. Such activities qualify as profiling under art. 4(4) of GDPR due to their automated nature and the inclusion of several personal data. Profiling inherently raises concerns about potential discriminatory outcomes as it involves processing data that might reflect intimate personal aspects, such as health, preferences, interests, economic stability, reliability, location or movements of a particular individual[28].

Under the GDPR framework, such profiling activities are assessed to ensure compliance with fundamental rights. When automated decisions significantly impact individuals (e.g., affecting creditworthiness), art. 22 establishes safeguards, mandating explicit consent or legal necessity and providing the right to contest automated outcomes. The critical balancing required here evaluates the proportionality and necessity of profiling against the backdrop of the data subject's fundamental rights and freedoms.

Indeed, according to recital 71, the specific risks may jeopardise the legitimate interests and rights of the data subject, in particular by taking into account the potential discriminatory effects against natural persons on the grounds of racial or ethnic origin, political opinions, religion or beliefs, trade union membership, genetic status, health or sexual orientation.

Therefore, again according to that recital, appropriate safeguards must be provided and fair and transparent processing must be ensured with due regard for the data subject, in particular by using appropriate mathematical or statistical procedures for profiling and by applying appropriate technical and organisational measures to minimise the risk of errors[29].

the data subject's performance at work, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements, where it produces legal effects concerning him or her or similarly significantly affects him or her. However, decision-making based on such processing, including profiling, should be allowed where expressly authorised by Union or Member State law to which the controller is subject, including for fraud and tax-evasion monitoring and prevention purposes conducted in accordance with the regulations, standards and recommendations of Union institutions or national oversight bodies and to ensure the security and reliability of a service provided by the controller, or necessary for the entering or performance of a contract between the data subject and a controller, or when the data subject has given his or her explicit consent. In any case, such processing should be subject to suitable safeguards, which should include specific information to the data subject and the right to obtain human intervention, to express his or her point of view, to obtain an explanation of the decision reached after such assessment and to challenge the decision. Such measure should not concern a child. In order to ensure fair and transparent processing in respect of the data subject, taking into account the specific circumstances and context in which the personal data are processed, the controller should use appropriate mathematical or statistical procedures for the profiling, implement technical and organisational measures appropriate to ensure, in particular, that factors which result in inaccuracies in personal data are corrected and the risk of errors is minimised, secure personal data in a manner that takes account of the potential risks involved for the interests and rights of the data subject and that prevents, inter alia, discriminatory effects on natural persons on the basis of racial or ethnic origin, political opinion, religion or beliefs, trade union membership, genetic or health status or sexual orientation, or that result in measures having such an effect. Automated decision-making and profiling based on special categories of personal data should be allowed only under specific conditions».

[28] E. Gil González-P. Paul De Hert, *Understanding the legal provisions that allow processing and profiling of personal data—an analysis of GDPR provisions and principles*, in *Era Forum,* 19, Berlin/Heidelberg, 2019, 597 ss.

[29] S. Wachter - B. Mittelstadt - L. Floridi, *Why a right to explanation of automated decision-making does not exist in the general data protection regulation*, in *International Data Privacy Law* 7.2, 2017, 76 ss.

It is worth noting that recitals, while not part of the operative provisions of specific legislation, are nonetheless incorporated into regulations[30], typically found in the preamble of legal documents such as EU regulations or international treaties to explain the purpose, objectives, and context of the law.

Although recitals do not create enforceable rights or obligations[31], they serve as tools for an "authentic interpretation" by providing insights into the drafter's intent[32]. Courts and legal practitioners often use recitals to resolve ambiguities within the operative provisions, aligning the application of the law with its intended purpose. This interpretive role gives recitals a *de facto* legal effect, reinforcing their importance for understanding and applying legislation. For these reasons, recital 71 is an important instrument to clarify GDPR's provisions.

That being said, the question referred for a preliminary ruling related explicitly to the automated calculation of a probability rate based on personal data concerning a person and their ability to honour a loan in the future. Such a decision produces significant legal effects on the person since the action of the client of the credit scoring company (i.e., the "third party") - to whom the probability result is transmitted - will suffer decisive legal effects, in the sense that an insufficient probability rate will, in almost all cases, lead to a refusal to grant the requested loan[33].

Under this perspective, the calculation of such a rate must therefore be qualified as a decision that produces with respect to a data subject's legal effects concerning them or similarly significantly affects them within the meaning of art. 22(2) GDPR. The latter gives the data subject the "right" not to be subject to a decision based solely on automated processing, including profiling. This provision enshrines a prohibition in principle, the violation of which does not need to be asserted individually by such a person.

[30] The legal doctrine has long discussed the legal value of recitals. Klimas and Vaiciukaite were puzzled by the extensive use of these instruments in European law: «it is claimed that while EC recitals have no legal value and cannot be the cause of derogation from an operative provision, they nevertheless create legitimate expectations (such as would defeat an operative provision). This is also strange. Recitals are supposed to be general statements. General statements are not something which ordinarily are recognized as giving rise to legitimate expectations. But also recitals in general (for instance, in contract law) are, well, recitals, not operative provisions and it is hard to fathom how they could give rise to positive obligations or defeat operative clauses. Thus, the doctrine surrounding recitals in EC law is mystifying. It is either irrational or so complicated as to amount to the same thing.». T. Klimas-J. Vaiciukaite, *The law of recitals in European Community legislation*, in *ILSA Journal of International & Comparative Law*, 15, 2008, 61 ss.

[31] In fact, the CJEU has affirmed multiple times that recitals cannot directly create rights and duties, see Case C-136/04, *Deutsches Milch-Kontor v Hauptzollamt Hamburg-Jonas*, EU:C:2005:716; Case C-134/08, *Hauptzollamt Bremen v J. E. Tyson Parketthandel*, EU:C:2009:229. M. den Heijer-T. van Os van den Abeelen-A. Maslyka, *On the use and misuse of recitals in European union law*, in *Amsterdam Law School Research Paper*, 3, 2019.

[32] According to Humphreys et al., recitals are important as the European Court of Justice makes frequent references to them as a support tool to establish the purpose of normative provisions. L. Humphreys-C. Santos-L. Di Caro-G. Boella-L. Van Der Torre-L. Robaldo, *Mapping recitals to normative provisions in EU legislation to assist legal interpretation*, in *Legal Knowledge and Information Systems*, 2015, IOS Press, 41 ss.

[33] S. Bastigkeit Ericstam, *AI in the Workplace: Regulating Explainability and Consent in Algorithmic Management,* in K. Prifti-E. Demir-J. Krämer-K.Heine-E.Stamhuis (eds), *Digital Governance. Information Technology and Law Series*, The Hague, 2024.

As follows from the combined provisions of art. 22(2) of the GDPR and recital 71[34] of that regulation, the Court of Justice stated that the adoption of a decision based solely on automated processing is authorised only in the cases referred to in the aforementioned article, i.e., where such a decision is necessary for the conclusion or performance of a contract between the data subject and a data controller within the meaning of point (a), or where it is authorised by the law of the Union or of the Member State to which the data controller is subject under point (b), or is based on the data subject's explicit consent under point (c)[35].

On this last point, some scholars suggested to pay attention to this point, since the debtor's consent may be given without being aware of it, for example, by signing forms or documents that the applicant signs without due care, either because they are vulnerable[36] or because of a tendency to underestimate the consequences of such an act, or the necessity of the signature to continue with the credit application which, in the applicant's belief, they hope will be successful.

In the cases referred to in art. 22(2)(a) and (c) of that Regulation, the data controller shall implement at least the data subject's right to obtain human intervention, to express their opinion, and to contest the decision. What is more, in the case of the adoption of a decision based solely on automated processing, such as that referred to in art. 22(1) of the GDPR, on the one hand, the data controller is subject to additional information obligations under art. 13(2)(f) and art. 14(2)(g) of that Regulation. On the other hand, the data subject enjoys, by art. 15(1)(h) GDPR, the right to obtain from the data controller, inter alia, «meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject[37]».

The aforementioned information and the data subject's access rights are consistent with the recognition of the right to an explanation and thus with the purpose pursued by art. 22 of the GDPR. It is to protect individuals against risks to their rights and freedoms arising from the automated processing of personal data, such as profiling[38]. Stressing the purpose of art. 22 invokes a sense of protection for the data subjects.

On the other hand, according to the author, in circumstances such as the present case, in which three parties with different interests are involved, namely the profiled applicant, the profiling agency, and the bank granting the loan, if the restrictive interpretation of art. 22 GDPR were to be accepted, there would be a risk of circumvention of art. 22 GDPR itself and, consequently, a gap in the legal protection of the weaker party, namely the person subjected to automated processing. The restrictive interpretation considers the calculation of the probability rate only as a preparatory

[34] G. De Gregorio–S. Demková, *The constitutional right to an effective remedy in the digital age: a perspective from Europe,* in C. van Oirsouw-J. de Poorter-I. Leijten-G. van der Schyff-M. Stremler-M. De Visser (eds), *European Yearbook of Constitutional Law 2023,* The Hague, 2024, 223 ss.

[35] CJEU, C-634/21, *SCHUFA* (2023), § 53.

[36] M. Girolami, *La scelta negoziale nella protezione degli adulti vulnerabili: spunti dalla recente riforma tedesca*, in *Rivista di Diritto Civile*, 2023, 854 ss; S. Kirwan, *Between a knock at the door and a knock to your score: re-thinking 'governing through debt'through the hopeful 'imaginaries' of UK debtors*, in *Journal of cultural economy* 14, 2021, 159 ss.

[37] CJEU, C-634/21, *SCHUFA* (2023), § 56.

[38] CJEU, C-634/21, *SCHUFA* (2023), § 52.

act, whereas only the act adopted by the third party can, i.e., the credit institution, be qualified as a "decision" within the meaning of art. 22(1) GDPR.

On the contrary, in the author opinion, what is assumed is only adherent to what happens during the automated decision-making process, where the mathematical calculation of probability is decisive for the definitive result on creditworthiness, which the applicant credit institution may use to grant money or not.

Even if this were not the case, the person subject to the profiling activity would not be able to access the information to defend themselves since the information is not in the bank's possession but is owned by the company that collects the information and processes it to obtain the result. On the other hand, in light of the statistical calculation being an integral part of the automated decision, there would be a correct attribution of liability on the part of the profiling agency: on the one hand, it is liable to the applicant by the unlawful processing of the data under art. 82 GDPR[39], while from a contractual point of view, it is liable for the relationship with the bank requesting the service of calculating the probability of fulfillment rate.

According to the author, even following a different argumentative logic, in the light of recital 71 of the GDPR, the same conclusion is reached: the data controller, i.e., the profiling agency, must use mathematical or statistical procedures suitable for profiling. It is also obliged to take appropriate technical and organisational measures to correct any errors or biases in the information used to ensure the security of personal data. These measures must consider the potential risks to the interests and fundamental rights of the individual concerned and prevent discriminatory effects against them[40].

It is up to the Verwaltungsgericht Wiesbaden to verify the terms under which art. 31 BDSG is consistent with art. 22 GDPR regarding the adoption of a decision based exclusively on automated processing on the basis of the interpretation developed by the Court of Justice[41].

Thus, according to art. 22(1) GDPR, «the automated calculation by a company providing business information of a probability rate based on personal data relating to a person and concerning that person's ability to meet payment commitments in the future constitutes an "automated decision-making process concerning natural persons" within the meaning of that provision, if the conclusion, performance or termination of a contractual relationship with that person by a third party, to whom that probability rate is disclosed, depends decisively on that probability rate»[42].

[39] A. B. Menezes Cordeiro, *Civil liability for processing of personal data in the GDPR*, in *European Data Protection Law Review*, 5, 2019, 492; R. Strugala, *Art. 82 GDPR: strict liability or liability based on fault?,* in *European Journal Privacy Law and Technologies*, 2020, 71; E. Tosi, Unlawful Data Processing Prevention and Strict Liability Regime Under EU GDPR, in The Italian Law Journal, 2021, 874 ss.

[40] According to K. Lagenbucher, «there is a fundamental tension between the [AI Act] Proposal's policy goal to protect fundamental human rights and its risk-based philosophy». K. Langenbucher-P. Corcoran, *Responsible AI Credit Scoring–A Lesson from Upstart.Com*, in *Digital Finance in Europe: Law, Regulation, and Governance*. *De Gruyter*, 2022; see also K. Langenbucher, *Responsible AI-based credit scoring–a legal framework*, in *European Business Law Review*, 31.4,2020.

[41] A. Aza, *Scores as Decisions? Article 22 GDPR and the Judgment of the CJEU in SCHUFA Holding (Scoring) in the Labour Context* in *Industrial Law Journal*, 53, 2024, 840 ss.

[42] CJEU, C-634/21, *SCHUFA* (2023).

3. Advocate General De La Tour's conclusions in the CK case on the relationship between access to information and protection of trade secrets

Another interesting case worth commenting is the CK case[43], which concerned a person who was denied the conclusion or an extension of the contract period by a mobile phone company, regarding a monthly payment of a mere EUR 10 (ten) sum, on the justification that the consumer lacked sufficient financial capacity. The plaintiff's alleged insufficient solvency was determined based on an automated credit assessment by the credit rating company, which was positive. In this litigation narrative there is a further disturbing aspect: this daily life case regards a small amount of the contract for which a credit rating was requested about the continuous payment of a very small sum. As a first consideration, one might ask whether a credit scoring procedure can be imposed for a derisory transaction and whether this entails an imbalance between securing creditworthiness and aggravating the stigma towards the less fortunate and those in serious financial difficulty. In addition, owning a mobile phone line is nowadays an essential service, as it was a landline in past years. Considering the small number of mobile companies, we might wonder what would happen if neither of them were willing to enter into a contract with the same individual based on this kind of assessment: would this person be completely cut off from communications?

While this consideration may concern the social aspects of credit scoring, the repercussions of a legal nature are addressed here. In this regard, art. 15(1)(h) gives the data subject the right to access information concerning him to verify that it is meaningful, accurate, and true. The referring court expressed suspicion about the authenticity of that information, because although the information provided to the applicant attributed to her high creditworthiness, her profiling indicated that she was insolvent even in her financial capacity to pay a sum of at least EUR 10. There is thus a contradiction between, on the one hand, the information provided to the consumer about her data processed and the logic used in the automatic assessment carried out and, on the other hand, the conclusion that the telephone operator drew from the rating assigned.

Therefore, a further critical issue arises: the possibility of legal protection for the logic employed in the credit scoring program by intellectual property rules such as trade secrets. But what does that logic consist of? According to the plaintiff, it would include the personal data of the data subject processed in the context of determining the factors, how this was done, and whether these data were weighed. Together with these must be included the essential parts of the algorithm on which the automated decision-making process is based, including the mathematical formula into which they can be entered, the steps by which that formula leads to that rating, and the understandable explanation of all the values used in that formula, in particular those which are not directly taken from stored information relating to the data subject. Additionally, relevant information shall be included to establish the correlation between the information processed and the valuation made, including an indication and

[43] Opinion of Advocate General De La Tour, Case C-203/22, C*K, Dun & Bradstreet Austria GmbH, Magistrat der Stadt Wien,* 12 September 2024.

adequate description of the valuation functions of all values used in such formula, an explanation of the information necessary to establish the correlation between the information and the valuation in the case of periodic valuations, and a presentation of the index functions used.

The other party invoked the existence of a trade secret under art. 2 part 1 of Directive 2916/943 to protect the algorithm and deny access to the logic used in the automated decision-making process[44].

In this dispute, the referring court observes that invoking industrial secrecy would make access to the information provided for by art. 15 GDPR impossible. Industrial secrets protection would prevent verifying information accuracy and comprehensibility and exercising rights under art. 22(3) GDPR and art. 47 of the Charter of Fundamental Rights of the European Union.

Thus, there would be a conflict between the right of access under art. 15, the right of explanation under art. 22 GDPR, and the right of third parties to the protection of algorithmic processes and the related black box.

The decision in this case could have important legal consequences beyond the specific ruling. It would complement the SCHUFA precedent of the Court of Justice of the European Union on a relevant issue, namely what is meant by «significant information about the logic used» in the context of an automated decision-making process using a black box in relation to the protection of trade secrets about the conduct of the decision-making process itself and thus the logic used.

According to the Advocate General, "significant information" within the meaning of art. 15(1)(h) GDPR must not only be clear and accessible but also accompanied by explanations that enable it to be understood. It is all truer when providing the data subject with information in a highly technical field, such as the interpretability of credit scoring systems. In that sense, such a provision offers the data subject a genuine right to obtain explanations as to the operation of the mechanism underlying an automated decision-making process to which that data subject was subject and the result to which that decision led. Recital 71 GDPR explicitly provides that an explanation of the decision must be issued following such an assessment.

In addition, the data subject must be able to verify the accuracy of the personal data concerning them and of the information concerning the logic used within the framework of an automated decision-making process. Furthermore, they must have the possibility of verifying that there is coherence and an objectively verifiable causal link between, on the one hand, the method and criteria used and, on the other hand, the result achieved by the automated decision. The information disclosed must enable the data subject to check whether it is true and whether the automated decision in question is indeed based on accurate information.

Recalling its case law (Case C-268/21, judgment of 2 March 2023, *Norra Stockholm Bygg*), the Court of Justice reiterates that a national court may consider that the personal data of the parties or third parties must be communicated to it to be able to consciously balance, in compliance with the principle of proportionality, the interests

[44] U. Mylly, *Transparent AI? Navigating between rules on trade secrets and access to information*, in *IIC-International Review of Intellectual Property and Competition Law* 54, 2023, 1013 ss.

at stake, namely access to its own data used on the one hand and industrial confidentiality on the other. The result of that balancing allows the national court to authorize the full or partial disclosure to the other party of the personal data thus disclosed if it considers that such disclosure does not go beyond what is necessary to ensure the effective enjoyment of the rights that individuals derive from art. 47 of the Charter of Fundamental Rights of the European Union concerning the right to an effective remedy. Such a principle may also apply to the information referred to in art. 15(1)(h) of the GDPR, even when it competes with the rights under art. 2(1)(1) of Directive 943/2016.

The Advocate General concludes that in the case of subjecting a person to an automated decision-making process as understood by art. 22 GDPR, meaningful information on the logic used, including profiling, concerns the method and criteria used by the data controller. They must be concise, easily accessible, understandable, and formulated in simple and clear language. They must also be sufficiently complete and contextualized to enable that person to verify their accuracy and whether there is a coherence and an objectively verifiable causal link between, on the one hand, the method and criteria used and, on the other hand, the result reached by the automated decision in question, so that the latter can be challenged knowingly by the data controller according to art. 15(1)(h) GDPR.

On the contrary, the data controller is not obliged to disclose complex technical information, such as instructions in a programming language, which would not be understood by laypeople who possess no specific expertise. Therefore, the Advocate General considers the disclosure of the algorithm used in the automated profiling process excludable.

4. The right to technical interpretability and AI automated decision-making

In our opinion, the Advocate General's solution is not satisfactory, and additional considerations are necessary.

First, the right to explanation is not stated in GDPR only, but also in Convention 108+, which is the only binding international legal instrument on the protection of personal data[45]. Convention 108+ applies to all personal data processing activities without limitation to sectoral distinctions. It includes data processing in justice, combating crime, defense, public safety, and state security. This is in contrast to the EU's GDPR, which has specific exclusions for activities such as state security and certain criminal justice matters[46]. Unlike older iterations or other frameworks, it no longer allows countries to exempt entire categories of data processing, such as those related to state security,

[45] C. Gallese, *Legal Aspects of AI in the Biomedical Field. The Role of Interpretable Model*s, in B. Carpentieri-P. Lecca (eds) *Big Data Analysis and Artificial Intelligence for Medical Sciences*, Hoboken, 2024, 339 ss.; C. De Terwangne, *Council of Europe convention 108+: A modernised international treaty for the protection of personal data*, in *Computer Law & Security Review* 40, 2021.

[46] However, Convention 108+ is not a self-executing treaty, so implementing legislation is needed, while GDPR does not need implementing laws.

from the Convention's protections. The text does include specific exceptions to ensure that vital public interests like combating crime, state security, or maintaining judicial independence are not hampered. However, these exceptions are narrowly tailored and do not amount to full exemptions for specific data processing categories.

Traditionally, the Convention focused on automated processing of personal data. Convention 108+ now also includes non-automated processing, provided the data is part of a structured, accessible, and retrievable set of information. Examples include paper-based registers, directories, and structured files, which must comply with the Convention's protections if they meet these criteria[47].

In the explanatory note of art. 10 of the Convention, credit scoring is explicitly cited: «Data subjects should be entitled to know the reasoning underlying the processing of their data, including the consequences of such a reasoning, which led to any resulting conclusions, in particular in cases involving the use of algorithms for automated decision-making including profiling. For instance, in the case of credit scoring, they should be entitled to know the logic underpinning the processing of their data and resulting in a "yes" or "no" decision, and not simply information on the decision itself. Without an understanding of these elements there could be no effective exercise of other essential safeguards such as the right to object and the right to complain to a competent authority». This convention is particularly important as it is not only applicable to EU Member States but also to other countries and it is still open to non-signatories members.

Secondly, we advocate for the recognizing of the "right to technical interpretability"[48] as a fundamental right, because, due to technical limitations, employing inherently interpretable models is the only way to protect citizens in high-risks AI applications. Interpretability means employing white boxes (ante-hoc models, glass-box approaches[49]) that are technically transparent, as opposed to black-boxes. In the heated debate on AI explainability, the doctrine, case law, and legislation have not theorized the existence of a right imposing the use of a specific model type from a technical point of view: AI providers and users are free to choose their preferred model.

However, in our opinion, if we consider the systematic interpretation of EU and international legal frameworks surrounding high-risk AI systems, a strong case can be made for establishing interpretability as a legal and ethical standard in this field, and in other sensitive domains as well (e.g., healthcare). High-risk systems that significantly affect individuals' rights and freedoms must be transparent and understandable to ensure accountability. Interpretability allows both the users (e.g., the bank employee) and those affected by these systems (e.g., the consumers) to understand how decisions are made, which is essential for upholding legal standards and protecting fundamental rights, without the need to disclose trade secrets or the algorithm itself.

In contrast, black-box AI systems - those whose internal processes are opaque and not easily understood, even by experts - should be used with caution. These systems

[47] C. De Terwangne, *Council of Europe convention 108+,* cit.

[48] C. Gallese, *The AI Act proposal: a new right to technical interpretability*? In *arXiv preprint arXiv:2303.17558*, 2023, forthcoming in Milan University Press.

[49] A. Holzinger-M. Plass-K. Holzinger-G.C. Crisan-C.M. Pintea-V. Palade, *A glass-box interactive machine learning approach for solving np-hard problems with the human-in-the-loop*, in *Creat. Math. Inform.* 28, 2019, 121 ss.

should only be employed in scenarios where decisions can still be fully evaluated based on factors other than the AI's output, such as on the basis of a human assessment. Relying solely on black-box outputs in critical decisions, especially in high-risk areas like healthcare, law enforcement, or financial services, presents serious risks to fairness, transparency, and accountability.

The definition of "causability"[50] by Holzinger et al. focuses on the essential relationship between AI systems and their users, in particular on how well an explanation supports causal understanding within a given context[51]. This definition assumes the inherent necessity of a causal model that links AI decisions to a framework comprehensible by a human expert to ensure transparency, efficiency, and user satisfaction. On the other hand, Ploug et al.'s perspective diverges by shifting the focus toward contestability[52], focusing on the possibility for patients (or users) to challenge or contest the AI's outputs, which represents a broader view of accountability. Unlike causability, Ploug et al. do not prescribe specific requirements for explainability, which could make their approach more flexible but potentially less grounded in standardized frameworks for interpretability.

These two different approaches are part of a broader debate in AI explainability[53], among which the question is whether the emphasis should lie on precise, causally grounded models tailored to experts or on creating systems open to contestation by different types of stakeholders.

In our opinion, the very possibility of exercising informed consent – the essence of personal autonomy - is compromised when individuals cannot understand how their data is being used or how decisions about them are made. This lack of transparency surely affects informed consent according to GDPR, but it also undermines the ability to challenge decisions that are based on automated decision-making processes (the contestability, as mentioned by Ploug), and even prevents consumers from knowing when they are being systematically discriminated in the first place. In fact, when decisions are generated by a black-box system, it is nearly impossible for an affected individual to appeal or dispute those outcomes, as they have no insight into how or why the decision was made.

Moreover, the absence of interpretability in AI systems directly threatens the exercise of several fundamental rights. For instance, the right to a fair trial can be compromised if consumers have not enough information to file for a case or to defend themselves; the right to self-determination is eroded when decisions impacting employment, credit, or healthcare are made by systems whose logic is inaccessible to the individual; and the right to non-discrimination is also at significant risk, as AI systems can inadvert-

[50] Defined as «as the extent to which an explanation of a statement to a human expert achieves a specified level of causal understanding with effectiveness, efficiency and satisfaction in a specified context of use».

[51] A. Holzinger-G. Langs-H. Denk-K. Zatloukal-H. Müller, *Causability and explainability of artificial intelligence in medicine*, in *Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery*, 9(4), 2019.

[52] T. Ploug-S. Holm, *The four dimensions of contestable AI diagnostics-A patient-centric approach to explainable AI* in *Artificial Intelligence in Medicine*, 107, 2020.

[53] The whole debate on AI explainability and interpretability is too extensive to be summarized in the present work.

ently perpetuate biases embedded in their training data[54]. Without transparency, it is difficult to detect or rectify discriminatory practices, a circumstance that undermines equality and fairness.

Given these concerns, it is clear that black-box systems should only be permissible in situations where their sole outputs do not determine the outcome of a decision. In such cases, there must be strong safeguards in place, including meaningful human oversight[55] and the consideration of other non-AI-based factors. This ensures that decisions remain accountable and can be scrutinized for fairness, accuracy, and compliance with human rights standards.

Ultimately, the lack of technical interpretability in AI systems presents significant barriers to justice, equality, and transparency. Since high-risk AI systems become increasingly integrated into daily decision-making processes that impact fundamental rights, interpretability must become the standard. This will ensure that automated systems remain accountable and that individuals retain the ability to challenge and understand the decisions that affect them. For this reason, we believe that there is room in the current EU legal system to theorize the existence of a right to technical interpretability.

Having explored the implications of art. 22 GDPR, it's time to turn our attention to art. 86 AI Act.

5. Is a remedial coexistence between art. 22 GDPR and art. 86 AI Act possible?

Art. 86 AI Act[56] plays a similar role to art. 22 GDPR and recognises the right to an individual explanation for the benefit of any person who has been affected by a decision made by the deployer based on the results of a high-risk AI system. The article provides that citizens who were affected by legal or similar significant effects in a way which that they consider to have a negative impact on their health, safety or fundamental rights, have the right to obtain - from the person in charge of the deployment -

[54] C. Gallese et al., *Investigating Semi-Automatic Assessment of Data Sets Fairness by Means of Fuzzy Logic,* in *2023 IEEE Conference on Computational Intelligence in Bioinformatics and Computational Biology (CIBCB)*. IEEE, 2023.

[55] Keeping in mind that «The controller cannot avoid the Article 22 provisions by fabricating human involvement. For example, if someone routinely applies automatically generated profiles to individuals without any actual influence on the result, this would still be a decision based solely on automated processing», Working Party 29, *Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679*, 2017.

[56] The text of art. 86 reads: «1.Any affected person subject to a decision which is taken by the deployer on the basis of the output from a high-risk AI system listed in Annex III, with the exception of systems listed under point 2 thereof, and which produces legal effects or similarly significantly affects that person in a way that they consider to have an adverse impact on their health, safety or fundamental rights shall have the right to obtain from the deployer clear and meaningful explanations of the role of the AI system in the decision-making procedure and the main elements of the decision taken. 2.Paragraph 1 shall not apply to the use of AI systems for which exceptions from, or restrictions to, the obligation under that paragraph follow from Union or national law in compliance with Union law. 3.This Article shall apply only to the extent that the right referred to in paragraph 1 is not otherwise provided for under Union law.».

clear and meaningful explanations on the role of the AI system in the decision-making process and on the main elements of the decision taken.

The article provides for an exception in the case of AI systems employed in critical infrastructures, that is those intended to be used as safety components in the management and operation of critical digital infrastructure, road traffic, or in the supply of water, gas, heating or electricity. Such systems are essential to public safety and economic stability and ensure the very survival of the population. Disclosing sensitive information about how AI systems operate within these critical infrastructures could inadvertently expose vulnerabilities, making them targets for cyberattacks or sabotage that could represent a risk for life. For example, detailed explanations of AI decision-making processes in these systems could reveal weaknesses in algorithms or operational dependencies, which malicious actors could exploit to disrupt essential services. In addition, if the deployers of high-risk AI systems were required to provide detailed, case-by-case explanations for decisions, it could create operational delays, legal disputes, or administrative burdens that might affect the efficient functioning of these systems.

Legislators have applied the principle of proportionality in crafting this exception, as the harm caused by requiring individualized explanations could outweigh the benefits of having an explanation. In these contexts, a clear explanation at the individual level might not be as feasible or as necessary as it would be for other high-risk AI systems impacting health, employment, or finances. Therefore, legislators recognized that the public interest in maintaining the safety and reliability of critical infrastructure outweighs the individual's right to a detailed explanation in these specific contexts.

The text of art. 86 of Regulation EU 1689/2024 appears innovative, but the protections granted by this provision remain insufficient[57]. Our critique of art. 86 of Regulation EU 1689/2024 is caused by a fundamental issue in the allocation of responsibility for providing explanations to individuals affected by decisions made using high-risk AI systems. While the article is a decisive step in granting individuals the right to obtain "clear and meaningful" explanations of the role of AI in decision-making as opposed to the mild art. 22 GDPR, we argue that the protections it offers remain unsatisfactory due to a significant gap in accountability.

Under the article, the responsibility for responding to individuals' requests for explanations is placed solely on the deployer of the AI system, that is the entity that implements and uses the system in practice. This means that the deployer is tasked with addressing concerns from affected individuals and providing the required explanations. However, this approach excludes the provider of the AI system, the entity that develops, designs, or supplies the underlying algorithm and methodology on which the system operates. The exclusion of the provider from the duty to reply is problematic because a third-party deployer may not possess sufficient technical knowledge to fully explain how the AI system operates at a deeper, systemic level. Deployers, for instance, might only understand how the AI system is applied in a specific context, such as making hiring decisions, loan approvals, or resource allocations, but they may lack insight

[57] S. Wachter, *Limitations and loopholes in the EU AI Act and AI Liability Directives: what this means for the European Union, the United States, and beyond*, in *Yale Journal of Law and Technology*, 26, 2024, 693.

into the design choices, data collection practices, and training methods that constitute the core of the AI's decision-making process. Since the provider is the one responsible for creating the system and determining how data is collected and processed, excluding them from the obligation to provide explanations leaves a significant gap in transparency and accountability every time deployers and providers are different entities.

This gap can result in explanations that are incomplete or superficial, depriving individuals of meaningful insight into how decisions affecting their lives are made. For example, if an individual challenges an AI-based mortgage decision, the deployer may be able to explain how the system was applied in practice but may not be able to address deeper questions about potential biases in the algorithm or the fairness of its training data. Without access to this technical information from the provider, the individual's ability to challenge the decision or seek justice is significantly undermined.

We argue that responsibility for responding to individuals' concerns should be shared between the deployer and the provider. The deployer should explain the practical aspects of how the AI system was used in the specific context of the decision, while the provider should be required to disclose technical details about the algorithm's design, its data processing methodology, and safeguards to ensure fairness and compliance. This shared responsibility would ensure that individuals receive meaningful explanations, addressing both the practical and technical dimensions of the decision-making process.

Since art. 86 places the entire burden of explanation on the deployer, it risks creating an accountability gap that undermines the regulation's goals of transparency and fairness. Deployers may struggle to provide full explanations, while providers, who are often in the best position to explain the system's functioning, are not required to engage with individuals at all. This circumstance limits the protections granted to individuals, making it harder for them to understand and challenge decisions that negatively affect their rights, health, or safety.

Additionally, the boundary for application of art. 86 is strict. This article is applicable only to high-risk AI systems, and it is only triggered if the AI decision has a significantly adverse impact on the health, safety, or fundamental rights of the user[58]. This means that harmful non-high-risk systems are excluded by this provision, despite their impact might be equally significant. For example, with the widespread use of generative AI systems – some of which even posing systemic risks – more and more individuals are forced to interact with chatbots and other automatic systems that perform a preliminary screening their requests (e.g., client service, online credit applications), finding themselves without protection despite being significantly affected by the general purpose AI system's decision.

Regarding what fundamental rights fall within the scope of credit scoring, it is argued that processing data concerning a person's reputation and dignity makes this tool available to the subject of credit profiling. Incorrect reporting as a bad payer could have significant consequences on the reputation of the person being ranked, which should be solid and adherent to reality. The damaging effects of an erroneous ranking or one

[58] H. van Kolfschooten-J. van Oirschot, *The EU Artificial Intelligence Act: Implications for healthcare*, in *Health Policy*, 149, 2024.

based on fallacious data or for derisory figures could cause damages, even if the resulting misfortunes are not comparable to those of Jean Valjean, who found himself a convict for a piece of bread stolen out of hunger.

According to GDPR, data subjects have the right to request a review or reconsideration of the automated decision, and they can ask for human intervention; in the case of an explanation request, if the answer obtained by the operator is not satisfactory, to whom can the subject person requesting the explanation turn? In the writers' opinion, there are three possibilities of appeal:

1. if, in the criticised automated decision, the requesting party finds a case of inadequate data processing within the meaning of the GDPR, the requesting party may appeal to the national supervisory authorities (art. 77 GDPR);
2. if the supervisory authority fails to address a complaint or respond in a timely manner, individuals can lodge a complaint against said authority to the courts of the Member State where the supervisory authority is based (art. 78 GDPR);
3. the ordinary courts are on the ground that the unlawful processing of personal data violates fundamental rights[59] (arts. 79 and 82 GDPR).

For issues that involve cross-border processing or interpretation of EU law, appeals can also be escalated to the CJEU.

One may wonder whether art. 86 competes with the remedy under art. 22 GDPR since the latter expressly refers to decision-making processing in the sense that it produces and enforces a decision having direct or indirect effects on the data subject. Nonetheless, the answer would seem to be negative, since it is only art. 86 that explicitly recognises that the explanation must be clear and meaningful, whereas the current text of art. 22 GDPR establishes «at least the right to obtain human intervention by the controller, to express one's opinion and to contest the decision» by the person subject to the automated decision[60]. Apparently, therefore, two distinct rights could be considered to be coexisting: art. 22 GDPR recognising the right to human intervention in data processing and art. 86 absorbing the right to request clear and meaningful explanations of the decision-making process for those parts of the latter that are not linearly explicable.

In addition, another difference is that art. 22 GDPR only refers to decisions taken on personal data only, while anonymized data are excluded. On the contrary, art. 86 AI Act has a broader scope, since it refers to any high-risk system, regardless of the data employed for its training, testing, validating, or those in the input and output. Therefore, even decisions made based on aggregated data or historical data, that affect a person or a group of persons despite not employing their personal data, must be explained. For example, if a bank decides to deny credit not to a specific customer but to an entire group of customers, based on the determinations of an algorithm that

[59] For example, under the Italian criminal code, the unlawful personal data processing might constitute a criminal offense.

[60] For an analysis of art. 22 GDPR and AI, see the works of Prof. Pagallo. U. Pagallo, *Algoritmi e conoscibilità*, in *Rivista di filosofia del diritto*, 2020, 9.1: 93 ss.; U. Pagallo, *Algo-rhythms and the beat of the legal drum*, in *Philosophy & Technology*, 2018, 31.4: 507-524. See also M. Palmirani et al., *Interpretabilità, conoscibilità, spiegabilità dei processi decisionali automatizzati*, in: *XXVI lezioni di Diritto dell'Intelligenza Artificiale*, Torino, 2021, 66 ss.

examined national statistics, an explanation must be provided to affected individuals.
Art. 86 also closely correlates with other GDPR provisions. Arts. 13(2)(f) and 14(2)(g) GDPR explicitly address automated decision-making, including profiling, when it produces legal or similarly significant effects on individuals. These provisions require data controllers to inform individuals about a) the existence of automated decision-making, b) the logic involved in these decisions, c) the significance and potential consequences of such processing for the individual. Thus, both frameworks target automated processes that impact individuals in legally or materially significant ways, but while the GDPR limits its focus to the use of personal data, the AI Act applies more broadly to high-risk AI systems, whether or not personal data is involved.

6. The comparative case-law following the *SCHUFA* ruling

In Austria, the subject of the assessment of the Bundesverwaltungsgericht (BVwG) is whether the automated creditworthiness determination procedure and whether such a decision falls under the discipline of art. 22 GDPR concerning access to the explanation of the automated decision. Applying the principles elucidated by the judgment of the Court of Justice of the European Union *SCHUFA* (C-634/21 OQ/Land Hessen), the Federal Administrative Court ruled that the automated calculation of a probability value by a credit information agency, based on personal data, is an «automated individual decision» when a third party relies on that value to establish, implement or terminate a contract with the person concerned.

In the present case, the BVwG held that the probability value provided by the holder to the energy supplier was decisive for the refusal to conclude a contract with the data subject, thus constituting an automated decision with significant legal effects within the meaning of art. 22 of the GDPR.

The BVwG also rejected the data controller's argument that the credit score was only a preparatory calculation, as this interpretation could circumvent art. 22 of the GDPR. In addition, the federal administrative courts ruled that none of the exceptions in art. 22(2) GDPR applied to the case, rendering the automated processing unlawful. The data controller also violated the principles of "lawfulness" and "fairness" under art. 5(1)(a) of the GDPR.

In Germany, the Landgericht Traunstein (LG Traunstein) ruled that art. 22(1) of the GDPR only applies when an automated decision has «legal effects» on the data subject, such as in the case of a contract rejection. Citing the EU Court of Justice, he clarified that an agency credit score only falls under art. 22 if it is the only criterion used in the decision-making process.

The court also clarified that data controllers do not bear the burden of proof for all GDPR requirements but only for the lawfulness of the processing. Therefore, the subject had to prove that the holder had violated art. 22(1) but failed to provide sufficient evidence. The legal process, in its fairness, also allowed the holder to prove that the subject had recently concluded contracts, disproving the idea of discrimination based on credit score. The Landgericht also rejected the allegation of discrimination, stating that age, gender, or address were not considered in the calculation of credit scores. As there was no evidence of a breach of the GDPR or harm suffered, the art. 82's claim was dismissed. The court concluded that the data subject's request for access to the data was satisfied and that the data controller could protect its trade secrets under art. 15(4) of the GDPR. On those grounds, the case was finally dismissed.

Those rulings are important as they clarify the boundaries of GDPR, however, they do not adequately consider systemic issues of discrimination. For example, as shown by multiple computer science works[61], even when "age, gender, or address" are not directly employed in a machine learning system, the algorithm can infer those characteristics by analysing strictly correlated dataset attributes. As recognized by legal scholarship[62], despite inferences can be as harmful as the personal data they refer to, in the era of big data and social media there is still a need to protect citizens from harmful inferences.

In the United States[63], on the one hand, there was—and it remains relevant today—a deep controversy regarding the presence of bias. Access to credit became an issue linked to the Civil Rights Movement[64], as racial elements were considered in credit profiling.

From a regulatory point of view, the Fair Credit Reporting Act of 1970, and later the amendments contained in the Equal Credit Opportunity Act of 1974, were enacted to ban the use of race, sex, and other personal traits in lending.

On the other hand, these laws prohibited financial and credit institutions from using information that could profile applicants in a discriminatory way. However, lenders were still able to use information indirectly related to these prohibited characteristics, such as postcodes, which revealed the social and racial background of applicants, including their ethnic origins[65]. This circumstance effectively preserved the influence of race in lending decisions[66].

As a result, a paradoxical effect has emerged: the use of statistical models and black-box algorithms[67] has not eliminated racial discrimination but has instead made it more challenging to identify.

[61] A. Fabris, *Measuring fairness under unawareness of sensitive attributes: A quantification-based approach*, in *Journal of Artificial Intelligence Research*, 76, 2023, 1117 ss.

[62] S. Wachter-B. Mittelstadt, *A right to reasonable inferences: re-thinking data protection law in the age of big data and AI*, in *Columbia Business Law Review,* 2019, 494; D. Clifford-M. Richardson–N. Witzleb, *Artificial intelligence and sensitive inferences: new challenges for data protection laws* in M. Findlay–J. Ford-J. Seah–D. Thampapillai (eds), R*egulatory Insights on Artificial Intelligence,* Cheltenham, 2022, 19 ss.

[63] B. Kiviat, *Credit scoring in the United States,* in *economic sociology_the european electronic newsletter,* 21(1), 2019, 33-42; J. Lauer, *Creditworthy: A History of Consumer Surveillance and Financial Identity in America,* New York, 2017, *passim.*

[64] B. Kiviat, *Credit scoring*, cit.; J. Laurer, *Creditworthy,* cit.; G. R. Krippner, *Democracy of Credit: Ownership and the Politics of Credit Access in Late Twentieth-Century America*, in *American Journal of Sociology*, 123, 2017, 1 ss.

[65] L. Hyman, *Debtor Nation: The History of America in Red Ink,* Princeton, 2011, *passim.*

[66] E. Cohen-Cole, *Credit Card Redlining*, in *The Review of Economics and Statistics* 93, 2011, 700 ss.

[67] F. Pasquale, *The black box society: The secret algorithms that control money and information,* Cambridge, 2011, *passim.*

Some recent studies[68] have investigated the impact of algorithms on the approval of monthly mortgage applications and have found that the gap between white and black applicants in the approval of applications is decreasing[69]. One may wonder whether this result is due to lawsuits filed over issues of discrimination in access to credit[70]. These cases highlighted the "reverse redlining" effect of creating and utilizing minorities and identifying a trusted social network to induce them to take out mortgages with high rates. Indeed, such disputes were connected to the financial crisis triggered by subprime mortgages, which began in the late 1980s and 1990s and exploded in the 2000s. This crisis was preceded by a shift in the evaluation of credit scoring, which no longer focused on the borrower's actual ability to repay the loan but rather on the security of repayment by reliable customers. This assessment was separate from the evaluation of the risk associated with less reliable customers, who were not denied loans but were instead subjected to higher costs. Indeed, this different credit scoring evaluation «brings more people into the market and expands the definition of who is "creditworthy," but at the same time, it demarcates new moral boundaries, such as those between "prime" and "subprime" borrowers»"[71].

Also in the United States, credit scoring has been the subject of judicial litigation that has reached the highest levels of jurisdiction. The US Supreme Court[72], a key player in shaping the legal landscape, unanimously ruled that the Fair Credit Reporting Act (FCRA) does not grant absolute immunity to the federal government (and federal agencies) in the case of erroneous debt reporting that impairs credit scores, thus allowing the federal government to be held liable for reporting. Justice Neil Gorsuch said the FCRA allows consumers to sue anyone who intentionally or negligently provides false information, including government agencies. The law defines "person" as any individual, company, government, or agency, indicating that the federal government can be liable.

According to the US Supreme Court, the issue is resolved by deferring to the principle of representative democracy because the will of the people, expressed by Congress[73], was to provide a remedy when the federal government violates a person's right to accuracy in credit reporting.

[68] A. C. B. Garcia-M. G. P. Garcia, R. Rigobon, *Algorithmic discrimination in the credit domain: what do we know about it?,* in *AI & SOCIETY*, 39(4), 2024, 2059 ss., spec. 2079; E. Yu, *Banking trends discrimination in mortgage markets*, in *Banking Trends* 7, 2022, 2 ss.; M. Giacoletti-R. Heimer-E. G. Yu, *Using high-frequency evaluations to estimate discrimination: Evidence from mortgage loan officers,* in *Proceedings of Paris December 2021 Finance* Meeting *EUROFIDAI-ESSEC,* 2021.

[69] E. Yu, *Banking trends discrimination in mortgage markets*, cit., 4.

[70] These cases are: *Baltimore vs. Wells Fargo Bank; City of Memphis vs. Wells Fargo Bank; Adkins et al. v. Morgan Stanley, Barkley v. Olympia Mortgage.* All these cases addressed predatory loans in violation of the Fair Housing Act. L. B. Hearit, *JPMorgan Chase, Bank of America, Wells Fargo, and the financial crisis of 2008,* in *International Journal of Business Communication*, 55, 2018, 237 ss.

[71] B. Kiviat, C*redit scoring in the United States,* cit. 36.

[72] 601 U.S. 42 (2024).

[73] E. B. Wydra-B. J. Gorod-M. Becker-Cohen, *United States Department of Agriculture Rural Development Rural Housing Service v. Kirtz*, 2024.

7. Conclusions

The *SCHUFA* decision by the CJEU represents an important precedent in the case law interpretation art. 22 of the GDPR, and it highlights that transparency and accountability in automated decision-making processes is still an issue for large companies. The innovative aspect of this ruling is that it recognizes credit scores as decisions with legal effects, even when they serve as intermediary steps in a larger decision-making chain.

Subsequent case law shows the far-reaching implications of the SCHUFA precedent. The Austrian and German court decisions refine the application of art. 22 GDPR, giving nuanced interpretations of what constitutes an automated decision and the extent of data controllers' obligations. However, these rulings collectively point towards growing judicial recognition of the need to balance individual rights with the legitimate interests of businesses in protecting their proprietary algorithms, without adequately considering issues of systemic discrimination posed by harmful inferences.

The introduction of art. 86 in the AI Act represents a complementary approach to addressing the challenges posed by high-risk AI systems. While it shares similarities with art. 22 GDPR, its broader scope and explicit focus on clear and meaningful explanations potentially offer enhanced protection for individuals affected by AI-driven decisions. However, the limitations in its applicability to only high-risk systems and the ambiguity surrounding the definition of "significantly adverse impact" may restrict its effectiveness in certain scenarios.

The comparative analysis, including the U.S. Supreme Court's ruling on the Fair Credit Reporting Act, shows that the challenges associated with credit scoring and automated decision-making are global. The decision to allow liability for erroneous reporting, even for government agencies, reflects a growing international consensus on the importance of the accountability principle in credit reporting systems.

The legal framework on credit scoring and AI-driven decision-making systems will likely continue to develop within the Digital Strategy[74]. The tension between the right to explanation, protection of trade secrets, and the need for algorithmic transparency remains an important area for future legal and policy development. The concept of a "right to technical interpretability" can be seen as a possible solution to protect citizens' rights without compromising intellectual property, as inherently interpretable models in high-risk applications are able to give clear explanations of the logic involved in the decision-making process. In light of the jurisprudence on credit scoring and automated decision-making, recognizing the existence of a "right to technical interpretability" becomes even more important. This right, while not explicitly codified in current legislation, can be inferred from the spirit of existing regulations such as the

[74] The Digital Strategy represents the European Union's focus on data, such as on the protection of personal data and the harmonization of data sharing practices, has been a priority since the Maastricht Treaty (1993), which significantly deepened EU integration. After the Maastricht Treaty, the EU began to enact the regulation of data to balance the need for privacy with the free flow of information necessary for economic and social integration. As early as the 1995, the Database directive was enacted, followed by the Data Protection Directive the same year. For an examination of the Digital Strategy, see C. Gallese, *A first commentary to the proposal for a new Regulation on fair access and use of data (Data Act)*, in *Media Laws*, 3, 2022, 237 ss.

GDPR and the AI Act, as well as from the judicial interpretations provided by courts across jurisdictions.

The SCHUFA implicitly acknowledged the need for interpretability in those systems. Other case law, including the Austrian and German court decisions, further refines this concept and highlights the importance of clear explanations of automated decisions when they have legal or similarly significant effects on individuals. This trend in judicial reasoning supports the idea that technical interpretability should be a fundamental right, especially in high-risk AI applications like credit scoring, as black-box models are so opaque that it is barely impossible to reach true transparency[75].

The introduction of art. 86 in the AI Act represents a step towards codifying aspects of the right to technical interpretability. Since it codifies the requirement of providing "clear and meaningful explanations" for decisions made by high-risk AI systems, it acknowledges the necessity of making complex technical processes comprehensible to those affected by them, complementing and expanding the transparency principle that is found in many Digital Strategy provisions. However, the limitations in its applicability greatly undermine its legal impact, as harmful non-high-risk systems, such as those based on Generative AI[76], are excluded by this provision.

The ongoing doctrinal, judicial, and legislative developments in this field need to move forward with a different approach that safeguards citizens' rights instead of siding with corporate interests. As AI systems become increasingly integrated into decision-making processes, impacting fundamental rights, the legal framework must at least ensure that all companies employing automated systems - not only those producing high-risk systems - remain accountable to those affected by their decisions. Although trade secrets should be preserved, this cannot happen at the expense of consumers. It is important that case law is able to keep up with the latest technological developments (such as Generative AI) and understand their impact on citizens and the whole society.

[75] C. Gallese, *The AI Act proposal: a new right to technical interpretability?,* cit.

[76] C. Gallese, *Web scraping and Generative Models training in the Directive 790/19*, in *i-lex* 16.2 2023, 1 ss.