Credit scoring and transparency between the AI Act and the Court of Justice of the European Union*

Elena Falletti[1,†] and Chiara Gallese[2,*,†]

[1] *Università Cattaneo-LIUC, Corso Matteotti 22, 20153, Castellanza, Italy*
[2] *Università di Torino, Lungo Dora Siena 100, 10153, Torino, Italy*

Abstract

Credit scoring software has become firmly established in the banking sector as a means to mitigate defaults and non-performing loans. These software systems pose significant challenges related to their non-transparent nature as well as biases inherent in the data nurturing the machine learning. Despite the Artificial Intelligence Act Proposal not being enacted yet, legal precedents have begun to emerge, starting with the ruling of the Court of Justice of the European Union (Case C-634/21). This ruling acknowledges that individuals seeking bank loans have the right, under Article 22 of the GDPR, to demand an explanation regarding the decision-making process of such programs. This article aims to analyze the evolution of credit scoring software since the SCHUFA ruling and the entering into force of the Artificial Intelligence Act.

Keywords

Artificial Intelligence, Automated Decision Making, Credit Scoring

1. Introduction

Credit risk assessment has long been the subject of debate in both doctrine [1] and case law [2, 3, 4].

The notion of risk regards an evaluation of a creditor's trust in a debtor's capacity to pay their debts. This kind of evaluation is necessary to uphold the integrity of the financial market, encompassing both borrowers for their ventures and investors leveraging others' savings. In assessing the trustworthiness of credit seekers, databases are utilized to document debtors' reliability, given the frequent convergence of these roles.

Using automated decision-making systems marked a significant advancement, integrating data on historical reliability alongside probabilistic projections of future solvency [5].

The logic behind using such tools lies in the empirical observation that human actions tend to repeat. Considering this seriality, it is considered reasonable to calculate the probability of a given behavior's recurrence by a mathematical procedure embedded in the algorithm.

This scoring contains an element of behavioral analysis that could hide a social-ethical judgment [6], which is linked to the risk of default.

It is because the loan denial is justified based on the result of the credit scoring software; therefore, biases capable of negatively influencing the algorithmic procedure [7] could ambush in the performance of this operation [8].

However, the application of the credit scoring algorithm is justified by the fact that, at least in abstract terms, it should treat serialized situations uniformly, ensuring, at least in intention, the conformity of access criteria by linking them with the solvency of past debts.

At this early stage, the procedure plays a decisive role in specific contexts, enabling decisions based on probability parameters.

AIMMES 2024 | Workshop on AI bias: Measurements, Mitigation, Explanation Strategies, Amsterdam, March 20, 2024.
[1*] Corresponding author.
[†] Dr. Elena Falletti wrote sections 2, 3, and 4; Conclusions were written jointly; Dr. Chiara Gallese wrote the rest.
efalletti@liuc.it (E. Falletti); chiara.gallese@unito.it (C. Gallese).
0000-0002-6121-6775 (E. Falletti); 0000-0001-8194-0261 (C. Gallese).

There is thus an area that can be quantified by the percentage of accuracy between the result processed by machine learning and the reality principle [9], and this space may contain errors [10], biases [11], hallucinations [12], or discrimination [13] depending on the quality of the data with which the dataset used by machine learning was formed [8].

The practice of evaluating credit trustworthiness has been performed - before the advent of AI - by employing traditional techniques [14, 15], which have not been regulated as strictly as in the new AI Act. In Italy, for example, only a general discipline is found in the banking code, regulating only credit scoring performed by banks and financial institutions.

We might argue that credit scoring itself is a sensitive topic that has the potential to significantly impact the lives of citizens, especially the wealthy, whether AI or not. However, AI models' capacity to be inherently opaque on a very large scale, impacting millions of people at once, differentiates them from other techniques. For this reason, we will focus the scope of this article on AI models.

The first section of the article focuses on article 22 GDPR (General Data Protection Regulation) and its implications; the second deals with a recent judgment of the Court of Justice of the European Union (Case C-634/21, see Fig. 1); the third examines the topic in light of the AI Act proposal; and the last draws some conclusive remarks.

2. Credit scoring and the right to an explanation under Article 22 GDPR

As explained in the previous section, the person subjected to the automated predictive decision must be able to access the explanation of the process carried out by the algorithm, whether it is a result in credit matters or about areas in which the fundamental rights of the person involved are put at risk.

In current law, this right is recognized by Art. 22 GDPR.[16,17] At the same time, Art. 68c of the Artificial Intelligence Act serves as the concluding rule for all areas not addressed by the aforementioned Art. 22 GDPR [18], despite some differences in its text, which has not yet been published in its official version as of the time of writing.

As is well known, Art. 22 GDPR provides for the right of the person subject to the decision to be informed of the automated process. As a defense against this claim, the protection of trade secrets on how the algorithmic software works is invoked [19].

Credit scoring programs concern a sub-category of predictive software measuring social scoring [13]. Generally speaking, credit scoring is a rate that assesses financial reliability, i.e., the possible predictability of repayment of the loan or mortgage. It is a score processed 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 on their classification within a category of similar subjects according to their characteristics [20].

Under this perspective, scholars observe that the credit scoring system measures the prediction of a behavior [21], by placing the person concerned in a category of profiles with a similar score; therefore, this score will be decisive in denying or granting the request based on the strict assumption that in standardized situations behavior is serialized.

Nevertheless, it should be borne in mind that “a profile is not a person” [22]. This assertion is only apparently obvious since the serialized data collected and treated in machine learning, precisely because they are serialized, fail to grasp the essence of each individual, both in the positive and negative sense. Therefore, it is neither possible nor common sense to consider the actual person coincident with the profile derived from the projection of the combination of their data [23].

Thus, the request for access to the decision-making process by a hypothetical but plausible loan applicant who was denied money is well-founded [24] in two respects, i.e. both under Article 22 GDPR, which recognizes the right to an explanation, and under Article 17 GDPR, i.e. based on what actual information this result was processed by machine learning [25]. Further, such protections are reinforced by Article 8 of the Charter of Fundamental Rights of the European Union, according to which every person has the right to access and obtain rectification of the data collected concerning them. It is an effect of the right to protection of personal data relating to individuals. According to this principle, personal data collected must be processed under the principle of fairness for specified purposes and based on the consent of the person concerned or for a legitimate purpose provided for by law [26].

In the context of the balancing act between the protection of personal data from the collection activities necessary for machine learning related to the credit scoring programs and the exception constantly presented in court about the protection of industrial secrets [27], protected by Article 17(2) of the same Charter, it is the latter that is recessive concerning the request for transparency. Indeed,

transparency as to the functioning of the algorithmic activity is necessary for understanding the logics that govern the evaluative classification relative to the attribution of the solvability score. Otherwise, the purpose of the data protection principle and the necessity of algorithmic transparency, provided for by the GDPR and reaffirmed by the approved Artificial Intelligence Act Proposal and in the publication process, would be thwarted [28].

In this regard, the source code should be accessible in any situation where potential discrimination could emerge, both direct and indirect [30], since the exercise of the right of access, in defense of the dignity and reputation of the party, since being unfairly considered a bad payer is a severe injury to reputation [30], is deemed to prevail over the protection of trade secrets.

As stated by scholarly opinion [31], not knowing the source code prevents the algorithm's traceability, violating the minimum explanatory duty established by European sources, such as Article 22 GDPR itself or Article 68c of the AI Act.

In the specific context, it was explored whether it was possible to create a fully interpretable machine learning model. In 2018, a competition known as the Explainable Machine Learning Challenge [22], was launched to explain how models work transparently. Surprisingly, some participants responded by proposing a transparent and interpretable model, thus demonstrating that machine learning can be organized relatively and transparently [32]. This approach has also attracted interest in credit scoring, with specific studies [30] also promoted by credit institutions. Although these studies may come from parties directly involved in a conflict of interest, they deserve attention [6].

3. The decision of the Court of Justice of the European Union on credit scoring

The legal case decided by the Court of Justice of the European Union (EUCJ) started in Germany and concerned the processing of personal data by a private credit agency. This entity provided information on the creditworthiness of third parties, such as consumers to banks or loaning activities [33].

At the same time, the credit agency was the data controller, processed the personal data of the profiled persons, and compiled the scores to be provided to the applicant banks using statistical and mathematical methods.

The credit score assigned by the data controller was taken into account by the scoring agency's contractual partners, who used those results in their decision-making process to decide whether or not to grant a loan to the borrower. The bank refused the applicant's credit request. The refusal was based on the result of the private agency in charge.

Following this, the client requested access to the information concerning her based on Article 22 GDPR. The German national data protection authority rejected this request, allowing the claimant to obtain specific information on personal data but not on the functioning of the negative credit scoring calculation. The applicant claimed that this last part is the heart of credit scoring, claiming that it was a process protected by trade secrets. The applicant challenged the refusal in court.

According to the referring court, the core of the question was whether determining the probability of default rate constituted an automated process within the meaning of Article 22 GDPR(1) since this provision is oriented towards protecting (natural) persons from the discriminatory risks associated with purely automated decisions.

The question concerns at which stage of assessing the customer's creditworthiness fits the automated calculation process whether at the assessment stage based on data provided by the third party (i.e., the bank) to SCHUFA in the actual calculating phase.

In the first case, there would be a legal loophole in that SCHUFA would have to respond to the requesting data subject based on Article 15(1)(h) GDPR alone, but not based on Article 22(1), and this would amount to a lack of protection, since on the one hand the automated decision-making process takes place during the first phase.

On the other hand, the bank that requested the service and to which the probability rate is communicated cannot provide information on the automation of the service since it is an outsourced service.

Since Art. 22 GPDR and Recital No. 71 have a specific rationale concerning the protection of the user against the automation of decisions without human intervention, it must be examined how Art. 31 BDSG (Bundesdatenschutzgesetz – Federal Data Protection Act) has implemented such protection in German law and whether it is compatible with it.

In this respect, two perspectives would open up: on the one hand, Section 31 BDSG would consider only the use of the probability rate, but not its calculation, as an automated process, and again, there would be a lack of protection. On the other hand, if calculating that probability rate did not constitute an automated

decision-making procedure for natural persons, neither Article 22 GPDR nor Paragraph 1 nor the opening clause of Paragraph 2(b) could apply.

The referring Court's question concerns the definition of what is intended as an 'automated decision' within the meaning of Article 22 GDPR and how this applies to credit scoring.

The EUCJ states that for Article 22 to be applicable, three conditions must coexist, namely: 1. that a decision must be necessary; 2. that it must be 'based solely on automated processing, including profiling'; and 3. that it must produce 'legal effects [concerning the data subject]' or affect 'in a similarly significant way their person.

Concerning point (a), the definition provided in Recital 71, according to which the data subject has the right to opt out of the legal effects produced by a purely automated decision affecting them, such as the automatic rejection of an online credit application or online recruiting practices managed by algorithms [34].

Elaborated in these terms, the Court stated that the decision on credit scoring referred to in the reference for a preliminary ruling falls within the applicability of Article 22 GDPR para. 1, since that carried out by SCHUFA, is a profiling activity under Art. 4, point 4 of the GDPR, where by its very nature discriminatory results may emerge, given that it involves data on even intimate characteristics of a person, such as health, personal preferences, interests not always directly related to their behavior, such as professional performance, economic situation, reliability, location or movements of that individual [35].

All these situations may be subject to measurement or balancing in the light of fundamental rights.

After that, the question referred for a preliminary ruling explicitly relates to the automated calculation of a probability rate based on personal data relating to a person and concerning that person's ability to honor a loan in the future.

Such a decision produces significant legal effects on the person since the action of the credit scoring company's client (i.e., the 'third party') to whom the probability result is transmitted will suffer decisive legal effects. An insufficient probability rate will, in almost all cases, lead to a refusal to grant the requested loan.

Therefore, calculating such a rate qualifies as a decision concerning a data subject's legal effects concerning or significantly similarly affecting them within the meaning of Article 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 lays down a prohibition in principle, the breach of which does not need to be asserted individually by such a person.

Indeed, as is evident from the combined provisions of Article 22(2) of the GDPR and Recital 71 of that regulation, the adoption of a decision based solely on automated processing is authorized only in the cases referred to in that 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 authorized 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 provided for in point (c).

Some attention must be paid to this last point since the debtor's consent may be given without being aware of it, for example, by signing forms or forms where the applicant signs without due care, either because he is 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, he hopes will be successful.

In the cases referred to in Article 22(2)(a) and (c) of that Regulation, the controller shall at least implement the data subject's right to obtain human intervention, to express his 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 Article 22(1) of the GDPR, on the one hand, the data controller is subject to additional information obligations under Article 13(2)(f) and Article 14(2)(g) of that Regulation. On the other hand, the data subject enjoys, under Article 15(1)(h) GDPR, the right to obtain from the data controller, among other things, "meaningful information about the logic used and the significance and intended consequences of that processing for the data subject."

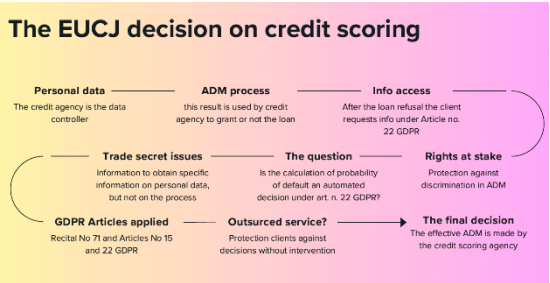

Figure 1 Summary of the decision

4. Credit Scoring in light of the AI Act

The European Commission finally released the first proposal for a harmonized legal framework on AI at the European level. This is a unique piece of legislation which is aimed at achieving four specific objectives:

- ensure that AI systems placed on the Union market and used are safe and respect existing law on fundamental rights and Union values;
- ensure legal certainty to facilitate investment and innovation in AI;
- enhance governance and effective enforcement of existing law on fundamental rights and safety requirements applicable to AI systems;
- facilitate the development of a single market for lawful, safe and trustworthy AI applications and prevent market fragmentation.

The enforcement mechanism of the proposal relies on a governance system at national level, building on already existing structures, and establishes a central cooperation mechanism through a "European Artificial Intelligence Board``.

The most important innovation of the proposal is the establishment of four risks categories for AI systems, in order to protect citizens' fundamental rights. The explanatory memorandum attached to the proposal, in fact, notes that ``The use of AI with its specific characteristics (e.g. opacity, complexity, dependency on data, autonomous behaviour) can adversely affect a number of fundamental rights enshrined in the EU Charter of Fundamental Rights ('the Charter'). This proposal seeks to ensure a high level of protection for those fundamental rights and aims to address various sources of risks through a clearly defined risk-based approach. With a set of requirements for trustworthy AI and proportionate obligations on all value chain participants, the proposal will enhance and promote the protection of the rights protected by the Charter: the right to human dignity (Article 1), respect for private life and protection of personal data (Articles 7 and 8), non-discrimination (Article 21) and equality between women and men (Article 23). It aims to prevent a chilling effect on the rights to freedom of expression (Article 11) and freedom of assembly (Article 12), to ensure protection of the right to an effective remedy and to a fair trial, the rights of defence and the presumption of innocence (Articles 47 and 48), as well as the general principle of good administration. Furthermore, as applicable in certain domains, the proposal will positively affect the rights of a number of special groups, such as the workers' rights to fair and just working conditions (Article 31), a high level of consumer protection (Article 28), the rights of the child (Article 24) and the integration of persons with disabilities (Article 26). The right to a high level of environmental protection and the improvement of the quality of the environment (Article 37) is also relevant, including in relation to the health and safety of people. The obligations for ex ante testing, risk management and human oversight will also facilitate the respect of other fundamental rights by minimising the risk of erroneous or biased AI-assisted decisions in critical areas such as education and training, employment, important services, law enforcement and the judiciary. In case infringements of fundamental rights still happen, effective redress for affected persons will be made possible by ensuring transparency and traceability of the AI systems coupled with strong ex post controls.

The risk categories are related to the degree (intensity and scope) of risk to citizens' safety or fundamental rights and are classified into four different categories for AI systems, among which the high-risk ones have to comply with many requirements and obligations. Taking inspiration from the product safety legislation, the classification of risks is based on the intended purpose and modalities for which the AI system is used, not only on their specific function. Depending on the national legal system, the qualification of high risk may have consequences over liability, such as that under art. 2050 of the Italian Civil Code. The proposal also draws up a list of prohibited AI systems that fall within the ''unacceptable risk" category [37].

The proposal, in Annex III, classifies AI systems employed for credit scoring as "high-risk". The decision to include such systems in this category was most likely drawn by the fact that financial institutions play an important social role by deciding to grant a mortgage or a financial instrument to citizens. In the end, they represent the only obstacle for less wealthy families to own a house or to afford essential means for their everyday life (e.g., being able to open their own business).

AI systems are known to perpetuate societal and historical biases, and there is no reason to believe that social scoring systems would be different: by providing safeguards, transparency measures, and precise obligations on AI providers and users, the

legislator intended to protect citizens from such systems.

In particular, the provisions about Data Governance and transparency are the most important. As known, an AI system is only as good as the data it relies on: if the data is flawed, the system will be biased. By providing an obligation to test the datasets for biases, the AI Act will ensure that credit scoring applications are not designed to discriminate groups or individuals, and by mandating clear instructions and information, it will put citizens in the position of being able to challenge the systems.

Although promising, the new regulation has not come as far as mandating full interpretability for AI systems. Therefore, some biases might still be present, and they might be difficult to detect when black boxes are employed.

5. Conclusions

The discourse presented herein, along with the data subject's rights to access their data, aligns with the acknowledgment of the right to explanation, thereby supporting the objectives of Article 22 of the GDPR. This article is designed to safeguard individuals from the potential hazards to their rights and freedoms posed by automated personal data processing, including profiling.

In scenarios where multiple parties with varying interests are engaged, such as the profiled individual, the profiling entity, and the lending institution, adhering to a narrow interpretation of Article 22 of the GDPR could inadvertently facilitate the evasion of the very protections it is meant to uphold, leaving the data subject—the most vulnerable party—without adequate legal defense. This narrow view regards the computation of the probability rate merely as a preliminary step, recognizing only the subsequent actions taken by an external entity, like a credit organization, as 'decisions' as defined by Article 22(1) of the GDPR [38].

Without an expansive interpretation, the individual subjected to profiling would be deprived of critical information necessary for their defense, as this data resides not with the bank but with the profiling company that collects and processes it. Conversely, recognizing the statistical evaluation as an inherent component of the automated decision-making process would rightly allocate responsibility to the profiling agency: it would be accountable for any unlawful data processing under Article 82 of the GDPR and contractually liable to the bank for the profiling service provided.

One may wonder whether such a principle may remain valid even after the AI Act's entry into force, the long process of which seems to have reached its final stages pending final publication. We note that Article 68c of the proposal signifies an enhancement of the right to explanation for automated decisions. This addition is applicable only where Union law, specifically Article 22 of the GDPR, does not already provide such a right. The provision introduces, beginning with its heading, an entitlement for data subjects to receive a 'clear and meaningful' elucidation of the decision-making process that involves them, particularly when high-risk AI systems are used, and the decision significantly impacts their fundamental rights.

Under Article 13(1) of the AI Act Proposal, individuals may request explanations from the deployer regarding the AI system's role, the pertinent input data, and the principal elements of the resulting decision. Nonetheless, exceptions may apply if the deployment of such AI systems is mandated by Union or national law, provided these exemptions uphold the core of fundamental rights and freedoms and are deemed necessary and proportionate within a democratic society.

In conclusion, we believe that the AI Act might have been slightly ''braver" by mandating more impacting transparency measures, such as interpretability, so that the reasoning behind the credit scoring classification would not have been hidden behind a black box.

Acknowledgements

This article was written with the contribution of the “SPIDER Project”, granted by the Cattaneo-LIUC University and the Project 101108151 — DataCom — HORIZON-MSCA-2022-PF-01. Partially funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Commission. Neither the European Union nor the granting authority can be held responsible for them.

References

[1] Ricci, Annarita. “Sulla segnalazione “in sofferenza” alla Centrale dei rischi e la dibattuta natura del preavviso al cliente non consumatore”. Contratto e impresa 1 (2020): 192-224.

[2] Cons. Stato, Sez. VI, Sent., 03/09/2009, n. 5198.

[3] Cass. civ., Sez. Un., Sent., 14/04/2011, n. 8487 (rv. 616973).
[4] Corte App. Palermo, Sez. III, Sent., 23/05/2023, n. 1003.
[5] Manes, Paola. "Credit scoring assicurativo, machine learning e profilo di rischio: nuove prospettive." Contratto e impresa 2 (2021): 469-489.
[6] A. Castelnovo, L. Malandri, F. Mercorio, M. Mezzanzanica, A. Cosentini, Towards fairness through time. In Joint European Conference on Machine Learning and Knowledge Discovery in Databases (pp. 647-663). Cham: Springer International Publishing, 2021.
[7] X. Dastile, T. Celik, M. Potsane, (2020). Statistical and machine learning models in credit scoring: A systematic literature survey. Applied Soft Computing, 91, 106263. doi: 10.1016/j.asoc.2020.106263
[8] A. Castelnovo, R. Crupi, G. Del Gamba, G., Greco, A. Naseer, D. Regoli, B. S. M. Gonzalez, (2020, December). Befair: Addressing fairness in the banking sector. In 2020 IEEE International Conference on Big Data (Big Data) (pp. 3652-3661). IEEE. Doi: DOI: 10.1109/BigData50022.2020.9377894.
[9] D. Pessach and E. Shmueli. "A review on fairness in machine learning". ACM Computing Surveys (CSUR), 55(3), (2022): 1-44.
[10] S. Charles, (2023). The Algorithmic Bias and Misrepresentation of Mixed Race Identities: by Artificial Intelligence Systems in The West. GRACE: Global Review of AI Community Ethics, 1(1).
[11] G. Pasceri. "Le scienze argomentative tra stereotipi e veri pregiudizi: la black box. Le scienze argomentative tra stereotipi e veri pregiudizi: la black box". (2023): 21-41.
[12] M. Dahl, V. Magesh, M. Suzgun, D. E. Ho,. (2024). Large legal fictions: Profiling legal hallucinations in large language models. arXiv preprint arXiv:2401.01301. URL: https://arxiv.org/abs/2401.01301.
[13] G. Cerrina Feroni, "Intelligenza artificiale e sistemi di scoring sociale. tra distopia e realtà." Il diritto dell'informazione e dell'informatica. (2023): 1-24.
[14] G. Spindler, "Algorithms, credit scoring, and the new proposals of the EU for an AI Act and on a Consumer Credit Directive". Law and Financial Markets Review 15.3-4 (2021): 239-261.
[15] G. L. Greco, "Credit scoring 5.0, tra Artificial Intelligence Act e Testo Unico Bancario". Rivista Trimestrale di Diritto dell'Economia. 2021.3 suppl. (2021): 74-100.
[16] Falletti, Elena. "Decisioni automatizzate e diritto alla spiegazione: alcune riflessioni comparatistiche." Il diritto dell'informazione e dell'informatica 36.2, marzo/aprile 2020 (2020): 169-206.
[17] Gallese-Nobile, C. (2023). Legal aspects of AI models in medicine. The role of interpretable models. Big data Analysis and Artificial Intelligence for Medical Science. Wiley.
[18] D. Schneeberger, R. Röttger, F. Cabitza, A. Campagner, M. Plass, H. Müller, A. Holzinger, The tower of babel in explainable artificial intelligence (XAI). In International Cross-Domain Conference for Machine Learning and Knowledge Extraction (pp. 65-81). (2023) Cham: Springer Nature Switzerland.
[19] F. Bravo, "Software di Intelligenza Artificiale e istituzione del registro per il deposito del codice sorgente." Contratto e impresa 4 (2020): 1412-1429.
[20] M. Pincovsky, A. Falcão, W. N. Nunes, A. P. Furtado, R. C. Cunha, Machine Learning applied to credit analysis: a Systematic Literature Review. In 2021 16th Iberian Conference on Information Systems and Technologies (CISTI) (pp. 1-5). 2021 IEEE. Doi: 10.23919/CISTI52073.2021.9476350.
[21] L. Ruggeri, "La dicotomia dati personali e dati non personali: il problema della tutela della persona nei c. dd. dati misti". Diritto di Famiglia e delle Persone. 2 (2023): 808-832.
[22] G. Gigerenzer, Perché l'intelligenza umana batte ancora gli algoritmi. Raffaello Cortina Editore, 2023.
[23] M. Hildebrandt, Defining profiling: A new type of knowledge?. Profiling the European citizen: Cross-disciplinary perspectives. Dordrecht: Springer Netherlands, 2008. 17-45.
[24] Bundesverwaltungsgericht (BVwG) (Austria), W252 2246581-1 , 29/6/2023.
[25] K. Demetzou, G. Zanfir-Fortuna, S. Barros Vale. "The thin red line: refocusing data protection law on ADM, a global perspective with lessons from case-law". Computer Law & Security Review 49 (2023): 105806.
[26] G. González Fuster, "The emergence of personal data protection as a fundamental right of the EU. Vol. 16. Cham: Springer Science & Business", 2014.
[27] E. Bayamlioğlu, "Machine Learning and the Relevance of IP Rights With an Account of

Transparency Requirements for AI." European Review of Private Law 31.2/3 (2023): 329-364.
[28] Gallese C., (2023). The AI Act Proposal: a new right to technical interpretability?. ArXiv preprint arXiv:2303.17558.
[29] J. Adams-Prassl, R. Binns, and A. Kelly-Lyth. "Directly discriminatory algorithms." The Modern Law Review 86.1 (2023): 144-175.
[30] V. Amendolagine, "La responsabilità aggravata della banca che agisce per un credito inesistente." Giurisprudenza Italiana 5 (2021): 1080-1083.
[31] Foa, Sergio. "Intelligenza artificiale e cultura della trasparenza amministrativa. Dalle "scatole nere" alla "casa di vetro?". Diritto Amministrativo. 2023.3 (2023): 515-548.
[32] C. Rudin and J. Radin. "Why are we using black box models in AI when we don't need to? A lesson from an explainable AI competition." Harvard Data Science Review 1.2 (2019): 10-1162.
[33] E. Falletti, "Alcune riflessioni sull'applicabilità dell'art. 22 GDPR in materia di scoring creditizio". Diritto dell'informazione e dell'informatica, (2024): 110-128.
[34] N. Rane, S. Choudhary and J. Rane. "Explainable Artificial Intelligence (XAI) approaches for transparency and accountability in financial decision-making." Available at SSRN 4640316 (2023). Doi: 10.2139/ssrn.4640316.
[35] J. Ochmann, L. Michels, V. Tiefenbeck, C. Maier, S. Laumer, (2024). "Perceived algorithmic fairness: An empirical study of transparency and anthropomorphism in algorithmic recruiting". Information Systems Journal. Doi: 10.1111/isj.12482.
[36] M. Girolami, "La scelta negoziale nella protezione degli adulti vulnerabili: spunti dalla recente riforma tedesca." Rivista di diritto civile 5/2023 (2023): 854-883.
[37] Gallese, C. (2022, November). Suggestions for a revision of the European smart robot liability regime. European Conference on the impact of Artificial Intelligence and Robotics (Vol. 4, No. 1, 29-35).
[38] E. Gil González, P. De Hert. "Understanding the legal provisions that allow processing and profiling of personal data—an analysis of GDPR provisions and principles." Era Forum. Vol. 19. No. 4. Berlin/Heidelberg: Springer Berlin Heidelberg, 2019.