JUS CIVILE

*CAMILLA TABARRINI**

Dottoressa di ricerca – Università Ca' Foscari Venezia

*GIOIA CALDARELLI**

Dottoressa di ricerca – Università Ca' Foscari Venezia

ARTIFICIAL INTELLIGENCE APPLIED TO THE PROVISION OF BANKING SERVICES. LATEST UPDATES TO THE EUROPEAN ACQUIS ON AUTOMATED CONSUMER CREDIT SCORING

1. – Originally, creditworthiness assessments (CWA) had only prudential relevance as it was conceived instrumental to the sound and prudent management of banking and financial institutions. [1]

Directives 2008/48/CE on credit agreements for consumers ("CCD") and 2014/17/EU on credit agreements for consumers in relation to residential properties ("MCD") were the first legal acts to look at CWA also as a tool of consumer protection to prevent over-indebtedness. Such extended regulatory perspective was later shared by the EBA in its Guidelines on loan origination and monitoring (EBA/GL/2020/06 – "LOGL"). [2]

---

* PhD "Diritto, Mercato e Persona" Ca' Foscari University, Venice; Directorate General for Consumer Protection and Financial Education, Bank of Italy. This contribution expresses exclusively the personal opinion of its authors and does not, in any case, bind the Bank of Italy.

[1] The general principle of sound and prudent management is enshrined in Article 5 of Consolidated Law on Banking (TUB). See *ex multis* BRESCIA MORRA, *Il diritto delle banche, Bologna, 2021, 209; Minneci, La verifica del merito creditizio: una valutazione a sua volta insindacabile?*, in *Riv. trim. dir. econ*., Suppl. n. 2 al n. 3, 2021, 354; INZITARI, *L'azione di massa per abusiva concessione di credito nella giurisprudenza della Cassazione*, in *Contr. impr.*, 2021, 1125 ss.; BENEDETTI, *La ridefinizione della fattispecie della concessione abusiva di credito ad opera della Cassazione*, in *Banca borsa tit. cred*., 2022, II, 173 ss.; INCUTTI, *Concessione abusiva del credito: profili di responsabilità e strumenti di tutela*, in *Riv. dir. impr.*, 2022, 221 ss. See also *Explanatory Note on the EBA's Comprehensive approach to loan origination*.

[2] In fact, to align financial institutions' CWA practices with consumer protection rules, the LOGL specify that the information

ISSN 2421-2563

Over the last years, rapid technological developments further changed the credit market facing both creditors and borrowers with new opportunities and risks.[3] A pivotal role in this ongoing market evolution is played by the ability of the latest machine-based systems to show unprecedented levels of autonomy, adaptiveness and ability to infer knowledge from the input they receive, also referred to as Artificial Intelligence (AI) systems under the recently adopted Artificial Intelligence Act (hereinafter AIA).[4]

In fact, although the business of assembling or evaluating consumer credit information have existed for decades,[5] Big Data and AI systems have sharply enhanced creditors capabilities to make creditworthiness inferences from both traditional and alternative data (e.g. data on geolocation, POS transactions and digital footprint)[6] as well as to translate into a numerical expression the probability of a consumer or business to repay a loan regularly and in full (i.e. credit score).

Therefore, it was in the context of the latest rise of so-called "cheap & fast" decision-making solutions, that concepts such as those of algocracy[7] and algorithmic surveillance[8] begun to surface. It is nowadays no-

---

underlying the CWA should "consider the current and prospective borrower's economic and financial situation and avoid inducing undue discomfort and excessive indebtedness" and that "creditors should have sufficient, accurate and up-to-date information and data to assess the creditworthiness and risk profile of the client before concluding a credit agreement".

[3] For further details on the risks and benefits associated with the ML systems, RABITTI, *Credit scoring via machine learning and responsible lending*, in *Riv. dir. banc*., 2023, 175. For an in-depth analysis of the notion of "creditworthiness" from a comparative perspective and of the critical interaction between policies of access to credit, financial inclusion, and responsible lending, N. VARDI, *Creditworthiness and 'responsible Credit': A Comparative Study of EU and US Law*, Brill/Nijhoff, 2022. In the United States, anti-discrimination regulations regarding credit have been in place for many decades. With special reference to credit transactions, the Fair Housing Act (FHA) of 1968 and the Equal Credit Opportunity Act (ECOA) of 1974 prohibit discriminatory practices based on race, religion, national origin, sex, disability, age and familial status. In the literature, specifically concerning advanced credit scoring systems, see P. HALL-B. COX-S. DICKERSON-A. RAVI KANNAN-R. KULKARNI-N. SCHMIDT, *A United States Fair Lending Perspective on Machine Learning*, in *Frontiers in Artificial Intelligence*, vol. 4, art. 695301, June 2021, 2.

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

[5] In the US the first legal act on the consumer credit reporting industry is the Fair Credit Reporting Act and dates back to 1970. For further details on the historic evolution of credit scoring practices see *Credit Scoring Approached Guidelines*, World Bank Group, 2019 available at https://thedocs.worldbank.org/en/doc/935891585869698451-0130022020/original/CREDITSCORINGAPPROACHESGUIDELINESFINALWEB.pdf.

[6] When talking about AI systems applied to credit scoring, we refer to the type of data used or to the type of models with which this data is processed, namely, the highly complex algorithmic models that can capture "non-linear" connections between data. For an in-depth look at machine learning techniques and their applications in credit scoring: A.A. NAIK-N.B. SHELOKAR, *Machine Learning Applications in Credit Scoring: Techniques and Applications*, CRC Press, 2021.

See also L. GAMBACORTA-Y. HUANG-H. QIU, J. WANG, *How do machine learning and non-traditional data affect credit scoring? New evidence from a Chinese fintech firm*, in *BIS Working Papers* n. 834, December 2019, 20, according to which scoring systems based on the use of machine learning and Big Data have a better predictive ability, compared with traditional systems, because they make better use of non-linear connections among variables. However, according to this study, the comparative advantage tends to be inversely proportional to the duration of the credit relationship. An example of a credit scoring model based on alternative data is the project presented by Experian Italia S.P.A. via the 2021 call for Proposals issued by the Bank of Italy's Milano Hub (the innovation centre designed to promote digital finance). Experian's digital credit scoring model is indeed powered by "digital data insights" such as the digital footprint left by the client when browsing websites or the metadata stored on mobile devices.

[7] The term "algocracy" was used for the first time by ANEESH, *Virtual Migration. The Programming of Globalisation*, Duke University Press Book, 2006. Alternatively referred to as 'big data scoring' or 'alternative data scoring': M. HURLEY-J. ADEBAYO, *Credit Scoring in the Era of Big Data*, in 18 *Yale Journal of Law and Technology* 148, 2016; H. WANG-C. LI-B. GU-W. MIN, *Does AI-based Credit Scoring Improve Financial Inclusion? Evidence from Online Payday Lending*, in (short paper), *ICIS* 2019 Proceedings 20 (https://aisel.aisnet.org/icis2019/blockchain_FinTech/blockchain_FinTech/20). For insights into ethical considerations and fairness issues in applying AI to credit scoring: S. BAROCAS-M. HARDT-A. NARAYANAN, *Fairness and Machine Learning: Limitations and Opportunities*, MIT Press, 2019; SILVEIRA, *Automated individual decision-making and profiling*, in *EU Law Journal* 2023, 8(2), 74.

[8] See Report on Artificial Intelligence: *Artificial Intelligence and Data Protection: Challenges and Possible Remedies* (Consulta-

ISSN 2421-2563

torious that algorithmic credit scoring could exacerbate risks of discrimination and distributional unfairness inherent in any statistical system.[9] This is especially true if AI's opacity, complexity, dependency on data and the risk of human overreliance are not properly addressed.[10] Hence, it is not surprising that the necessity to set boundaries to safeguard a number of fundamental rights potentially threatened by AI (e.g. human dignity (Article 1 EUCHR), respect for private life and protection of personal data (Articles 7 and 8 EUCHR), non-discrimination (Article 21 EUCHR), special groups' rights (Article 28 EUCHR)) is gaining more and more regulatory momentum.

The objective to promote a sustainable and human-centric technological development is at the core of the so-called industry 5.0.[11] However, as clearly stated also in the Draghi Report,[12] this growing regulatory production can multiply administrative burdens on companies and ultimately hinder technological innovation and economic growth. This is especially true for cross-sectoral legal acts setting obligations that apply also to business sectors that are already strictly regulated.

In light of the above, the objective of this article is twofold: (*i*) to provide an overview of the latest regulatory and case law developments on automated credit-granting practices involving consumers (paragraph 2); and (*ii*) to draw and initial mapping of regulatory overlaps stemming from the newly introduced obligations for financial institutions that are providers or deployers of AI systems intended to be used to assess consumer creditworthiness (paragraph 3).

To this end, the next paragraph will describe the evolution of European and international debate on automated decision-making and its current regulatory regime under the General Data Protection Regulation (Reg. (EU) 2016/679, hereinafter GDPR), the Directive (EU) 2023/2225 of the European Parliament and of the Council of 18 October 2023 on credit agreements for consumers and repealing Directive 2008/48/EC (hereinafter CCD2) and the AIA. The article will then move on to highlight the overlaps as well as the differences between the transparency requirements applicable to automated credit scoring practices under the GDPR, the CCD2 and the AIA. The analysis will conclude with the discussion of the main open questions that will need to be addressed in implementing the AIA.

---

tive Committee of the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, 25 January 2019 (T-PD(2018)09Rev)) 17; CEPEJ, *European Ethical Charter on the use of Artificial Intelligence in judicial systems and their environment*, adopted at the 31st plenary meeting of the CEPEJ (Strasbourg, 3-4 December 2018), 46 esp. fn. 58.

[9] For instance, models opacity and data bias: indeed, the cognitive bias incorporated in AI models can be systematically reproduced and this may compromise the validity of the model and the pureness of the results, creating a vicious cycle. See also AIA, Recitals 5 and 61. Also, in Machine Learning (ML) systems, while a properly representative dataset could minimise the risk of group's under or over representation, an inadequate one could generate a dangerous feedback loop where distortion in data selection can be confirmed and reinforced.

[10] See also Bonaccorsi Di Patti, Calabresi, De Varti, Federico, Affinito, Antolini, Lorizzo, Marchetti, Masiani, Moscatelli, Privitera, Rinna, *Artificial Intelligence in credit scoring. An analysis of some experiences in the Italian financial system*, in *Questioni di Economia e Finanza* (Occasional Papers) 721, Bank of Italy, Economic Research and International Relations Area. The paper, which provides insights on the adoption of (AI-ML) techniques by Italian financial intermediaries survey, is available in Italian at this link: https://www.bancaditalia.it/pubblicazioni/qef/2022-0721/QEF_721_IT.pdf.

[11] European Commission, *Industry 5.0* (https://research-and-innovation.ec.europa.eu/research-area/industrial-research-and-innovation/industry-50_en); European Commission, *ERA industrial technologies roadmap on human-centric research and innovation for the manufacturing sector*, 2024 available at ERA industrial technologies roadmap on human-centric research and innovation for the manufacturing sector – Publications Office of the EU (europa.eu).

[12] The future of European competitiveness, Part B – In-depth analysis and recommendations, September 2024, 317 available at https://commission.europa.eu/document/download/ec1409c1-d4b4-4882-8bdd-3519f86bbb92_en?filename=The%20future%20of%20European%20competitiveness_%20In-depth%20analysis%20and%20recommendations_0.pdf.

ISSN 2421-2563

2. – **2.1.** – The notion of algorithmic transparency in automated decision-making was originally conceived as a data protection issue and, from this perspective, have been thoroughly discussed over the last years. [13] Indeed, the so called "black box problem", earlier also referred to as the "scored society", [14] was first raised in 2015 from a philosophical perspective by Frank Pasquale who used this expression to indicate "a system whose workings are mysterious; [as] we can observe its inputs and outputs, but we cannot tell how one becomes the other". [15]

This notwithstanding, the first legislative provision on automated decisions dates to almost forty years earlier as it can be found in article 2 of the January, 6th 1978 French law on *informatique, aux fichiers et aux libertés* stating that "[*a*]*ucune décision de justice impliquant une appréciation sur en comportement humain ne peut avoir pour fondement un traitement automatisé d'informations donnant une définition du profil ou de la personnalité de l'intéressé*".

At the international level, a first legislative attempt to address automated data processing was made on 28 January 1981 with the original Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108). Indeed, Article 8 thereof provided for additional safeguards including the ability of any person "to establish the existence of an automated personal data file, its main purposes, as well as the identity and habitual residence or principal place of business of the controller of the file". [16]

In 1995 the European legislator introduced a similar provision in the first Directive on the protection of individuals with regard to the processing of personal data and on the free movement of such data (Directive 95/46/EC). Namely, Article 15 on "automated individual decisions" provided for data subjects' right "not to be subject to a decision which produces legal effects concerning him or significantly affects him and which is based solely on automated processing of data intended to evaluate certain personal aspects relating to him, such as his performance at work, creditworthiness, reliability, conduct, etc.". In 2016 this right flowed into Recital 71 and Article 22 GDPR.

These legislative attempts to regulate automated decisions were however fairly ignored for decades to the point where the right not be subject to automated decisions was even defined a "second-class data protection right". [17]

The first scholars to ever theorize the existence of a right to "receive an explanation for algorithmic decisions" were Goodman and Flaxman who, shortly after the repeal of Directive 95/46/EC and the adoption of

---

[13] M. HILDEBRANDT, *FAT* 20* (*Conference on Fairness, Accountability, and Transparency*, Barcelona, January 2020); Z. PAPACHARISSI (ed.), *A Networked Self and Human Augmentics*, in *Artificial Intelligence, Sentience*, Routledge, 2019; G. RESTA, *Governare l'innovazione tecnologica: decisioni algoritmiche, diritti digitali e principio di uguaglianza*, in *Politica del diritto*, 2019, 2, 199; UK Information Commissioner's Office (ICO), *Feedback request – profiling and automated decision-making* (2017) 19, and *Article 29 Working Party, Guidelines on Automated*; BURRELL, *How the machine 'thinks': Understanding opacity in machine learning algorithms*, in 1 *Big Data & Society* 1-2, 2016. See also B. LEPRI-J. STAIANO-D. SANGOKOYA-E. LETOUZÉ-N. OLIVER, *The Tyranny of Data? The Bright and Dark Sides of Data-Driven Decision-Making for Social Good*, in T. CERQUITELLI-D. QUERCIA-F. PASQUALE (eds.), *Transparent Data Mining for Big and Small Data*, in *Studies in Big Data*, Vol. 11, Springer, 2017, 12.

[14] D. KEATS CITRON-F. PASQUALE, *The Scored Society: Due Process for Automated Predictions*, in 89 *Washington Law Review* 1 10, 2014. See also J. VAN DIJCK, *Datafication, Dataism and Dataveillance: Big Data Between Scientific Paradigm and Ideology*, in *12 Surveillance & Society* 2, 2014, 197-208.

[15] G. HARMAN, *Prince of Networks: Bruno Latour and Metaphysics* (re.press 2009) 37 and mentioned by F. PAQUALE, *The Black Box Society. The Secret Algorithms That Control Money and Information* (HUP 2015) 4 and 222, especially fn 7.

[16] CETS 108 – Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (coe.int).

[17] I. MENDOZA-L.A. BYGRAVE, *The Right Not to be Subject to Automated Decisions Based on Profiling*, in T.E. SYNODINOU-P. JOUGLEUX-C. MARKOU-T. PRASTITOU (eds.), *EU Internet Law. Regulation and Enforcement*, Springer International Publishing AG, Cham, 2017, 77 e 80.

ISSN 2421-2563

the GDPR, argued that the combined reading of articles 13 (2)(f), 14(2)(g), 15(1)(h) and 22 GDPR enshrined controllers' duty to provide data subjects with "meaningful information about the logic involved" in automated decision making. [18]

Many legal scholars followed by discussing and further developing this interpretative assumption [19] while, on the legislative side, the Modernised Convention for the Protection of Individuals with Regard to the Processing of Personal Data of 18 May 2018 (so called Convention 108+) [20] expressly provided for data subjects' right to "to obtain, on request, knowledge of the reasoning underlying data processing where the results of such processing are applied to him or her" (Article 9) following the regulatory footsteps traced by the GDPR.

At the same, the European Parliament joined these efforts by adopting Resolutions of 16 February 2017 and of 12 February 2019 to promote human-centric AI by setting ethical rules to provide, *inter alia*, transparency of algorithmic decision-making [21] "to reduce the AI system's computations to a form comprehensible by humans; [and to equip advance robots] with a 'black box' which records data on every transaction carried out by the machine, including the logic that contributed to its decisions". [22]

2.2 – It is undisputed that a decision on a credit application based on the automated processing of personal data is potentially covered by Article 22 GDPR as it significantly affects data subjects access to fundamental services. Indeed, both Recital 71 GDPR and the explanatory note to Convention 108+ [23] exemplify the risks posed by automated decisions therein regulated as those affecting data subjects' ability to access credit.

---

[18] B. GOODMAN-S. FLAXMAN, *European Union regulations on algorithmic decision-making and a "right to explanation"*, in (2017) 38 *AI Magazine* 3 first presented at 2016 ICML Workshop on Human Interpretability in Machine Learning (WHI 2016), New York, NY. For an opposite point of view see 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 7 *International Data Privacy Law* 2 76, 2017.

[19] See for example G. MALGIERI-G. COMANDÈ, *Why a right to Legibility of Automated Decision-Making Exists in the General Data Protection Regulation*, in 7 *International Data Privacy Law* 4 243, 248, 2017; S. BAROCAS-A. D. SELBST, *Big Data's Disparate Impact*, in 104 *California Law Review* 671, 680, 2016; J. BURRELL, *How the machine 'thinks': understanding opacity in machine learning algorithms*, in 1 *Big Data & Society* 1-2, 2016; B. LEPRI-J. STAIANO-D. SANGOKOYA-E. LETOUZÉ-N. OLIVER, *The Tyranny of Data? The Bright and Dark Sides of Data-Driven Decision-Making for Social Good*, in T. CERQUITELLI-D. QUERCIA-F. PASQUALE (eds.), *Transparent Data Mining for Big and Small Data*, in *Studies in Big Data*, Vol. 11, Springer, 2017, 12; L. EDWARDS-M. VEALE, *Slave to the Algorithm? Why a 'Right to an Explanation' Is Probably Not the Remedy You Are Looking For*, in 16 *Duke Law & Technology Review* 18 39, 2017; M. ANNANY-K. CRAWFORD, *Seeing Without knowing: limitations of the transparency ideal and its application to algorithmic accountability*, in 20 *New Media & Society* 3 973-989, 2016; R. TAYLOR, *No Privacy Without Transparency*, in R. LEENES-R. VAN BRAKEL-S. GUTWIRTH-P. DE HERT (eds), *Data Protection and Privacy: The Age of Intelligent Machines*, Hart Publishing, 2017, 77; M. MATTIOLI, *Disclosing Big Data*, in 2 *Minnesota Law Review* 99 535, 2014; T. Z. ZARSKY, *"Mine your Own Business!": Making the Case for the Implications of the Data Mining of Personal Information in the Forum of Public Opinion*, in 5 *Yale Journal of Law and Technology* 1 45; A.D. SELBST-JULIA POWLES, *Meaningful information and the right to explanation*, in 7 *International Data Privacy Law* 4 233-242, 2017.

[20] Council of Europe, Modernised Convention for the Protection of Individuals with Regard to the Processing of Personal Data (Explanatory Report of June 2018 available at ES222664_PREMS 085218 GBR 2018 Convention 108 Web.pdf (europa.eu)).

[21] European Parliament resolution of 12 February 2019 on a comprehensive European industrial policy on Artificial Intelligence and robotics (2018/2088(INI)), §143.

[22] The European Parliament resolution of 16 February 2017 with recommendations to the Commission on Civil Law Rules on Robotics (2015/2103(INL), §12. The European Parliament Resolution of 12 February 2019 provided a comprehensive European industrial policy on Artificial Intelligence and robotics and affirmed that Artificial Intelligence (AI) has the potential to enrich our lives and further our capabilities, for both individuals and the common good. At the same time, it highlighted the need for a strong policy on how to maximize these benefits and minimize the risks for society and businesses. Specifically, these are the potential distortive effects related to the use of Artificial Intelligence to make decisions regarding people, in particular, whether to grant consumers access to credit.

[23] Council of Europe, Modernised Convention for the Protection of Individuals with Regard to the Processing of Personal Data (Explanatory Report of June 2018, §77.

ISSN 2421-2563

This notwithstanding, the legal debate continued on the extent to which automated CWA and credit scoring practices actually fall within scope of application of the general prohibition set by Article 22(1) GDPR. [24] Indeed, for Article 22(1) GDPR to apply, three cumulative conditions must be met: (*i*) there must be a 'decision'; (*ii*) the decision must be based solely on automated data processing or profiling; and (*iii*) it must legally or at least significantly affect data subjects.

The EUCJ recently addressed this interpretative question by deciding a case brought up by a consumer (OQ) who was refused a loan by a financial company following an insufficient credit score determined by a German third-party private company (Schufa). [25]

First, both the Advocate General (AG) and the EUCJ stated that a decision within the meaning of Article 22 GDPR encompasses any public or private opinion statement with a binding character producing factual or legal consequences. Hence, by affecting a data subject's ability to be granted credit, Schufa's score qualifies as a private decision producing significant effects on data subjects under Article 22(1) GDPR.

Second, the EUCJ clarified that the loan refusal amounts to a decision solely based on Schufa's score pursuant to Article 22(1) GDPR if the creditor's decision on the loan application strongly drew on the credit score. Although this is generally a question of fact that the EUCJ leaves for national courts to answer on a case-by-case basis, it offered interpretive guidance based on the factual information provided by the referring court. Namely, the EUCJ deemed Schufa score covered by Article 22 GDPR by adopting a substantial interpretative approach to safeguard data subjects' rights to be informed about the existence of an automated data processing and to obtain meaningful information regarding its underlying algorithmic logic, its significance and its envisaged consequences (Articles 13(2)(f), 14(2)(g) and 15(1)(h) GDPR). [26] In fact, although the financial company did not formally solely rely on the score transmitted by Schufa to make the final decision, empirical and statistical evidence suggested that a negative score was generally sufficient to lead to the refusal to grant credit. [27]

---

[24] Article 22 GDPR provides for the data subject's right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning them or similarly significantly affects them. This provision does not apply to solely automated decisions necessary for entering into/performing a contract, nor to automated decisions authorised by Union or National or based on a data subject's explicit consent. In any of these latter cases, data controllers must implement suitable safeguards for the data subject's rights that at least encompass the right to obtain human intervention from the controller, to express their point of view and to contest the decision.

[25] Namely, Schufa's business is to provide its contractual partners with scores expressing the probability regarding a person's future behaviour (such as the repayment of a loan) formulated on the assumption that an individual will behave similarly to someone from a group of people with comparable characteristics. EUCJ, Judgement of 7 December 2023, Case C-634/21. For a complete analysis of the EUCJ Judgment: D'Orazio, *Il credit scoring e l'art. 22 del GDPR al vaglio della Corte di giustizia*, in *La Nuova Giurisprudenza Civile Commentata*, n. 2, 1 marzo 2024, 410. See also, Falletti-Gallese, *Credit scoring and transparency between the AI Act and the Court of Justice of the European Union*, AIMMES, 2024; Pietrella-Racioppi, *Il credit scoring e la protezione dei dati personali: commento alle sentenze della Corte di giustizia dell'Unione europea del 7 dicembre 2023*, in *Rivista italiana di informatica e diritto*, 6, no. 1 (2024), 16-16; Fasano, L*'interpretazione estensiva della nozione di "decisione automatizzata" ad opera della Corte di giustizia: una prospettiva più ampia ma ancora fragili tutele per le libertà fondamentali*, in *Rivista italiana di informatica e diritto*, 6, no. 2 (2024), 15-15; Asymina 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*, 2024, available at https://doi.org/10.1093/indlaw/dwae035.

[26] In order to ensure a fair and transparent data processing, Articles 13 and 14 GDPR state that at the time when the personal data is obtained (either directly from data subjects or indirectly from third-party providers) data controllers must inform data subjects about, among other things, the existence of automated decision-making, including profiling, as referred to in Article 22(1) and (4) GDPR and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject. Furthermore, pursuant to Article 15 GDPR, this information is also to be provided by controllers upon the data subject's request. In this regard, see also EUCJ, Judgement of 7 December 2023, Case C-634/21, paras 57 and 66.

[27] EUCJ, Judgement of 7 December 2023, Case C-634/21, §60-62. For insights on how to overcome such interpretative assumption see below sub paragraph 3.2, esp. ft. 88.

ISSN 2421-2563

Third, the EUCJ found that, although falling within the general prohibition set by Article 22(1) GDPR, credit decisions could still be lawfully based on automated credit scores if it is: (a) authorised by EU or national legislation pursuant to Article 22(2)(b) GDPR; (b) in line with the requirements set by Articles 5 GDPR [28]; and (c) carried out under a legal basis set by Article 6 GDPR. [29] In this last regard, the EUCJ left it with the referring court to verify whether the national data protection law can be classified as a legal basis under Articles 6 and 22(2)(b) GDPR. If not, Schufa data processing would lack a legal basis, and the financial company credit decision would infringe upon the prohibition laid down in Article 22(1) of the GDPR. [30]

2.3. – When the CCD originally entered into force in 2008 Article 8 dealt with the obligation to assess the creditworthiness of the consumer, by generally providing for creditworthiness assessment to be carried out on the basis of sufficient information obtained from the consumer (where appropriate) and from the consultation of relevant databases (where necessary). In this case, Article 9(2) CCD also required for creditors to timely provide the consumer with free information on the database consulted.

Six years later, more detailed CWA provisions were introduced in the MCD. Indeed, pursuant to Recital 55 and Article 18 MCD, the CWA shall be carried out on the basis of information on the consumer's income and expenses and other financial and economic circumstances that is necessary, sufficient and proportionate. Moreover, unlike the CCD, under Article 18(5) MCD creditors are required to inform the consumer both ahead of the consultation of a database and once the data is obtained. Furthermore, MCD expressly provides for Member states to ensure that credit is only granted to consumers when the CWA indicates that the obligations stemming from the credit agreement are likely to be fully met.

Overall, neither the CCD, the MCD nor its original implementing guidelines on CWA [31] addressed the use of automated tools in the credit-granting process. The first reference to algorithmic CWA was indeed introduced in 2020 when the EBA published the LOGL as part of the Action Plan to tackle the high level of non-performing loans. Namely, LOGL expressly allow the use of automated models in the decision-making processes complying with the governance framework set therein. [32]

---

[28] Article 5 GDPR sets seven principles relating to the processing of personal data: (*i*) lawfulness, fairness and transparency; (*ii*) purpose limitation; (*iii*) data minimization; (*iv*) accuracy; (*v*) integrity and confidentiality; (*vi*) storage limitation; (*vii*) accountability.

[29] In this regard, the AG expressed the view that of the three legal basis provided for in Article 6(1) potentially applicable in a case such as that at issue in the main proceeding (i.e. performance of a contract, compliance with a legal obligation and pursue of a legitimate interest of the controller), only the legitimate interest basis actually fits. Among other arguments, according to the AG, the legal basis of the pursuit of a controller's legitimate interest could potentially cover a regulation of a business activity that, such as Schufa's credit scoring, can contribute to the stability of the financial system and could therefore amount to an interest worth protecting if there aren't any data-protection friendlier alternatives to pursue it. However, the AG also noted that since Article 6(f) GDPR provides for a balance of the conflicting interests of the controller and of the data subject, it does not allow for the adoption of national laws that, by authorising the use of scores in the financial sector, allow controllers's economic interests to take precedence over data protection rights, without leaving interpretative room to the particular circumstances of the individual case. In fact, according to consolidated EU case law "Member States cannot definitively prescribe, for certain categories of personal data, the result of the balancing of the opposing rights and interests, without allowing a different result by virtue of the particular circumstances of an individual case. Opinion of Advocate General Pikamäe delivered on 16 March 2023, §§ 68, 71, 73-74, 87. See also EUCJ Judgement of 19 October 2016, Breyer (C-582/14, EU:C:2016:779, paragraph 62).

[30] EUCJ, Judgement of 7 December 2023, Case C-634/21, §71.

[31] Guidelines on creditworthiness assessment (EBA/GL/2015/11) of 21 March 2016 to support the national implementation by Member States of the MCD, repealed by the LOGL as of 30 June 2021.

[32] Namely, in Section 4 the LOGL set out supervisory expectations for institutions when their lending activities involve the use of automated models in creditworthiness assessments and credit decision-making.

ISSN 2421-2563

In 2023 a recast text of the CCD was published (CCD2)[33] and the provision on consumer CWA was widely amended to introduce more detailed requirements. For example, as opposed to the former Article 8(1) CCD, Article 18 CCD2 now clarifies that the consumer CWA has to be "thorough", thus setting clear quality standards for creditors to meet before concluding a credit agreement.[34] Also, Article 18(1) of CCD2 currently stresses that "[…] [CWA] shall be carried out in the interest of the consumer, to prevent irresponsible lending practices and over-indebtedness […]". Furthermore, while maintaining the possibility for creditors to consult databases, Article 18 CCD2 goes further by prohibiting social networks from being considered as an external data source under the CCD2 and by requiring an appropriate verification of the information obtained in accordance with Article 18(3) CCD2, even "through reference to independently verifiable documentation" (where necessary).

In its recast version, the CCD now also expressly addresses the use of automated processing of personal data when carrying out CWAs. More specifically, the CCD2 complements the transparency rights enshrined in the GDPR by addressing two core AI use cases for the credit industry: the price personalization to targeted consumers or groups thereof and the CWA of consumer applying for a loan.[35]

Namely, when the price presented to consumers is personalised on the basis of automated processing of personal data (including inferred data), creditors and credit intermediaries are required to clearly display such information in both the pre-contractual forms and the actual offer, so that clients can take into account the potential risks in their purchasing decision.[36]

On the other hand, whenever the creditworthiness assessment involves automated data processing, pursuant to Recital 56 and Article 18(8) CCD2, consumers should be able to speak to someone in person so as to: (a) request and obtain from the creditor a clear and comprehensible explanation of the CWA, including the logic and risks involved in the automated processing of personal data as well as its significance and effects on the decision; (b) express their own point of view; and (c) request the creditor to review of the CWA and its consequent credit decision.

Furthermore, pursuant to Article 18(9) CCD2, when credit refusal is based on automated data processing, the creditor shall inform the consumer of their right to request the review of the CWA and describe the procedure for contesting the credit decision.

This notwithstanding, these consumers' rights never entail a "right to obtain credit".[37]

2.4. – The AIA was adopted in the pursuit of the "EU Strategy to shape the next Europe's decade and make our future fit for the coming digital age". In fact, the objective of the Regulation is to promote the uptake of transparent, non-discriminatory and human-centric AI (so called trustworthy AI).[38] To this end, the

[33] By 20 November 2025 Member States are to adopt and publish all the national provisions necessary to comply with the CCD2 to be then applied the following year. For a review of some of the most relevant provisions of the new Directive: TRAPANI, *La nuova Direttiva 2023/2225/UE sul credito al consumo: note in tema di educazione finanziaria, merito di credito e servizi di consulenza sul debito*, in *Le Nuove Leggi Civili Commentate*, n. 3, 1 maggio 2024, 754.

[34] Article 18(2) also acknowledges the role of credit institutions in the creditworthiness assessment process, by stating that "Member States shall ensure that credit intermediaries accurately submit the necessary information obtained from the consumer to the relevant creditor in accordance with Regulation (EU) 2016/679 to enable the creditworthiness assessment to be carried out".

[35] Recital 56 CCD2.

[36] Recital 46 CCD2 and Articles 10 (3)(m), 11(4)(h) and 13 CCD2.

[37] Recital 56 CCD2.

[38] Recital 1 AIA states that the "purpose of this Regulation is to improve the functioning of the internal market by laying down a

ISSN 2421-2563

AIA introduces a proportionate risk-based AI governance framework that provides stakeholders with entrepreneurial guidance towards the development, placement and use of AI systems that can stand the test of European fundamental values. [39]

Following the Brussel Effect, the AIA applies worldwide to providers of AI systems (including general-purpose AI models) that are either: (i) placed on the market or put into service in the Union; or (ii) producing outputs that are used in the Union. The AIA also applies to all deployers of AI systems located within the Union or deployers located in third countries but producing AI outputs used in the Union. [40]

Overall, the AIA sets four different regulatory regimes for AI systems, [41] depending on the intensity of the risks posed to persons' fundamental rights. Namely: (*i*) minimal-risk AI (e.g. spam filters) is allowed without specific restrictions; [42] (*ii*) limited-risk AI (e.g. generative AI, [43] chatbots and deep fakes) is allowed subject to minimum transparency obligations; [44] (*iii*) high-risk AI (e.g. credit scoring) is allowed subject to a set of

---

uniform legal framework in particular for the development, the placing on the market, the putting into service and the use of Artificial Intelligence systems (AI systems) in the Union, in accordance with Union values, to promote the uptake of human centric and trustworthy Artificial Intelligence (AI) while ensuring a high level of protection of health, safety, fundamental rights as enshrined in the Charter of Fundamental Rights of the European Union (the 'Charter'), including democracy, the rule of law and environmental protection, to protect against the harmful effects of AI systems in the Union, and to support innovation." In the same sense see also Article 1(1) AIA. Similarly, Recital 6 of the AIA stresses "the need to build trust, [as] it is vital for AI and its regulatory framework to be developed in accordance with Union values as enshrined in Article 2 of the Treaty on European Union (TEU), the fundamental rights and freedoms enshrined in the Treaties and, pursuant to Article 6 TEU, the Charter. As a prerequisite, AI should be a human-centric technology. It should serve as a tool for people, with the ultimate aim of increasing human well-being." These objectives follow those previously set by the European Council (Special meeting of the European Council of 1 and 2 October 2020 – Conclusions, EUCO 13/20, 2020, 6) and the European Parliament (Resolution of 20 October 2020 with recommendations to the Commission on a framework of ethical aspects of Artificial Intelligence, robotics and related technologies, 2020/2012(INL)).

[39] This assumption is clearly expressed in Recital 3 AIA and was also stressed in previous versions of the document by stating that the "proposal lays down obligation that will apply to providers and users of high-risk AI systems. For providers who develop and place such systems on the Union market, it will create legal certainty and ensure that no obstacle to the cross-border provision of AI-related services and products emerge. For companies using AI, it will promote trust among their customers. For national public administrations, it will promote public trust in the use of AI and strengthen enforcement mechanisms (by introducing a European coordination mechanism, providing for appropriate capacities, and facilitating audits of the AI systems with new requirements for documentation, traceability and transparency)." Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain Union legislative acts, Brussels, 21.4.2021, Com (2021) 206 Final, §3.4. On this topic see also MADIEGA, *Artificial Intelligence act, European Parliamentary Research Service (EPRS)*, in *PE 698.792*, November 2021.

[40] Article 2(1), AIA.

[41] In its final drafting, AI systems are defined by Article 3(1) AIA as a "machine-based system designed to operate with varying levels of autonomy and that may exhibit adaptiveness after deployment and that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments". Hence, since a key characteristic of AI systems within the meaning of the AIA is their capability to go beyond basic data processing by inferring knowledge from any given input, the Regulation should not cover AI tools that merely execute rules set solely by natural persons (Recital 12, AIA).

[42] In its Q&A of 12 December 2023 the European Commission defined minimal risk as that posed by a residual category of AI systems that "can be developed and used subject to the existing legislation without additional legal obligations". The European Commission also clarified that these AI systems represent the "vast majority of AI systems currently used or likely to be used in the EU fall into this category", and that in these cases AI may voluntarily choose to apply the requirements for trustworthy AI and adhere to voluntary codes of conduct. See *Artificial Intelligence – Q&As* (europa.eu).

[43] As clarified in Recital 99 of the AIA, Generative AI models are the most typical subset of general-purpose AI as they "allow for flexible generation of content, such as in the form of text, audio, images or video, that can readily accommodate a wide range of distinctive tasks", as opposed to so called narrow AI that performs in specific fields.

[44] According to Recital 27 of the AIA "[t]ransparency means that AI systems are developed and used in a way that allows appropriate traceability and explainability, while making humans aware that they communicate or interact with an AI system, as well as duly informing deployers of the capabilities and limitations of that AI system and affected persons about their rights". This, for ex-

ISSN 2421-2563

mandatory requirements over its entire lifecycle; (*iv*) unacceptable-risk AI (e.g. social scoring) is prohibited because contravening Union values. [45]

It follows that, with specific regard to AI-based scoring practices, the AIA sets a preliminary distinction between social and credit scoring.

Social scoring (i.e. the estimation of personal or personality characteristics over certain periods of time) [46] is prohibited inasmuch as it leads to either (or both): "(*i*) detrimental or unfavourable treatment of certain natural persons or groups of persons in social contexts that are unrelated to the contexts in which the data was originally generated or collected; (*ii*) detrimental or unfavourable treatment of certain natural persons or groups of persons that is unjustified or disproportionate to their social behaviour or its gravity". [47] Consequently, social scoring practices are apparently allowed if: (*i*) producing favourable effects (even disproportionate to the social behaviour) in contexts related or unrelated to those in which the data was originally generated/collected; (*ii*) producing unfavourable but proportionated effects in context related to those in which the data was originally generated/collected. Moreover, Recital 31 further clarifies that this "[social scoring] prohibition should not affect lawful evaluation practices of natural persons that are carried out for a specific purpose in accordance with Union and national law". [48] It is however worth mentioning that Annex III of the AIA does not list AI systems intended to be used for allowed social scoring practices in the list of high-risk AI systems. Hence, it remains unclear which regime should apply.

On the other hand, under the AIA, AI systems used to evaluate the creditworthiness of natural persons or establish their credit score are generally classified as high-risk, [49] unless used for the purpose of detecting fi-

---

amples, could result in pop-ups flagging the use of an AI system when interacting with humans. On the contrary, for AI systems posing specific transparency risks, such as chatbots, specific transparency requirements are imposed due to the risk of manipulation mitigated by ensuring users awareness when interacting with a machine. See *Artificial Intelligence – Q&As* (europa.eu).

[45] The adopted version of the AIA does not formally define social scoring practices but from Article 5(1)(c) it can be inferred that it is regarded as "the evaluation or classification of natural persons or groups thereof over a certain period of time based on their social behaviour or known, inferred or predicted personal or personality characteristics". On the difference between social and credit scoring see below sub para 5.2.

[46] Under the European Parliament's version of Article 3 AIA, social scoring was defined as the evaluation or classification of natural persons based on their social behaviour (i.e. the way a natural person interacts with and influences other natural persons or society), socio-economic status or known or predicted personal or personality characteristics (Artificial Intelligence Act. Amendments adopted by the European Parliament on 14 June 2023 on the proposal for a regulation of the European Parliament and of the Council on laying down harmonised rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain Union legislative acts (COM(2021)0206 – C9-0146/2021 – 2021/0106(COD)), Amendments 208-209 to Article 3 para 1 point 44k and point 44l). This wording was not replicated in the final version of the Act. Still, Recital 31 AIA currently describes social scoring as the evaluation or classification of natural persons or groups thereof based on multiple data points related to their social behaviour in multiple contexts or known, inferred or predicted personal or personality characteristics over certain periods of time. Contrary to the original proposal, social scoring is therefore prohibited if carried out not only by public authorities but also by private actors and also if concerning groups of natural persons.

[47] Article 5 (1)(c) AIA.

[48] With its amendments to Article 5(1a) the EU Parliament proposed to more generally stress that all the prohibitions set therein "shall not affect the prohibitions that apply where an artificial intelligence practice infringes other Union law". This proposal was not included in the final draft. See Artificial Intelligence Act. Amendments adopted by the European Parliament on 14 June 2023 on the proposal for a regulation of the European Parliament and of the Council on laying down harmonised rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain Union legislative acts (COM(2021)0206 – C9-0146/2021 – 2021/0106(COD)), Amendment 228.

[49] Article 6(2) and Annex III, §5(c) AIA. More generally, on the use of AI for credit scoring purposes see, for example, HURLEY-ADEBAYO, *Credit Scoring in the Era of Big Data*, in 18 *Yale J.L. & Tech.* 148; *Credit Scoring Approaches Guidelines*, World Bank Group, 2019 available at CREDITSCORINGAPPROACHESGUIDELINESFINALWEB.pdf (worldbank.org); *Understanding algorithmic decision-making: Opportunities and challenges*, European Parliamentary Research Service, March, 2019 available at

ISSN 2421-2563

nancial fraud (Annex III, §5(b) AIA) or for prudential purposes to calculate credit institutions' and insurances undertakings' capital requirements (Recital 58 AIA). [50]

Article 6(3) AIA provides for more general exemptions to the classification of AI systems as high-risk. Namely, an AI system listed in Annex III is exceptionally classified as not high-risk if it is alternatively or cumulatively intended to: (*i*) perform a narrow procedural task; [51] (*ii*) improve the result of previously completed human activity; [52] (*iii*) detect decision-making patterns or deviations from prior decision-making patterns and is not meant to replace or influence the previously completed human assessment, without proper human review; [53] (*iv*) perform a preparatory task to an assessment relevant for the purpose of the use cases listed in Annex III. [54] However, none of these exemptions apply to high-risk AI systems intended to be used for CWA or credit scoring purposes. Indeed, pursuant to Article 6(3) AIA, any "AI system referred to in Annex III shall always be considered to be high-risk where the AI system performs profiling of natural persons". Hence, since any form of CWA or credit scoring entails the processing of personal data to evaluate, analyse or predict, *inter alia*, aspects concerning that natural person's economic situation, such AI systems clearly fall within the definition of profiling within the meaning of Article 4(4) GDPR, [55] as also stated by the AG in the Schufa case. [56]

3. – In light of the above, financial institutions as well as credit reporting agencies that are providers or deployers of AI systems used to evaluate the creditworthiness of natural persons or establish their credit score are subject to (at least) the requirements set by the AIA, the GDPR, the MCD, the CCD (including its recast version).

EPRS_STU(2019)624261_EN.pdf (europa.eu); BÜCKER-SZEPANNEK-GOSIEWSKA-BIECEK, *Transparency, auditability, and explainability of machine learning models in credit scoring*, in *Journal of the Operational Research Society*, 2021, 73(1), 70-90; D. WUBE-Z. ESUBALEW-F. WELDESELLASIE-G. DEBELEE, *Deep Learning and Machine Learning Techniques for Credit Scoring: A Review*, in DEBELEE-IBENTHAL-SCHWENKER-MEGERSA AYANO, (eds) *Pan-African Conference on Artificial Intelligence*, vol. 2069, Cham, Springer, 2024; HAY-LE VESCONTE, *Financial Regulation*, in KERRIGAN (ed.), *Artificial Intelligence. Law and Regulation*, Edward Elgar Publishing Limited, 2022.

[50] Originally, considering the very limited scale of the impact and the available alternatives on the market, the Commission proposed to exempt from the high-risk classification AI systems "put into service by small scale providers for their own use", but such exemption did not make it to the final drafting. However, specific derogations for SMEs (including start-ups) providers and deployers are nonetheless provided for by Articles 62-63 AIA.

[51] According to Recital 53 AIA an AI system is intended to perform a narrow procedural task is for example "an AI system that transforms unstructured data into structured data, an AI system that classifies incoming documents into categories or an AI system that is used to detect duplicates among a large number of applications".

[52] According to Recital 53 AIA an example of AI system that only provides an additional layer to a human activity would be "AI systems that are intended to improve the language used in previously drafted documents, for example in relation to professional tone, academic style of language or by aligning text to a certain brand messaging".

[53] According to Recital 53 AIA "[s]uch AI systems include for instance those that, given a certain grading pattern of a teacher, can be used to check *ex post* whether the teacher may have deviated from the grading pattern so as to flag potential inconsistencies or anomalies".

[54] According to Recital 53 AIA this criterion, for example, "covers, inter alia, smart solutions for file handling, which include various functions from indexing, searching, text and speech processing or linking data to other data sources, or AI systems used for translation of initial documents".

[55] For the definition of profiling under the AIA see Article 3(52).

[56] In the words of the AG "the scoring carried out by SCHUFA is covered by the legal definition contained in Article 4(4) of the GDPR, since that procedure uses personal data to evaluate certain aspects relating to natural persons to analyse or predict aspects concerning their economic situation, reliability and probable behaviour". See Opinion of Advocate General Pikamäe delivered on 16 March 2023, §33.

ISSN 2421-2563

Such multi-layered regulatory framework makes it necessary, especially in highly regulated sectors such as the financial one, to assess and identify regulatory overlaps. Indeed, a clear outline of the interplay of all the relevant legal acts is pivotal to reach the AIA declared objective "to ensure consistency, avoid duplication and minimise additional burdens" on both providers and deployers of AI systems. [57]

Along these lines, the next paragraphs will draw an initial map of the main regulatory implications and overlaps both in terms of consumers' rights and creditors' obligations concerning the use of AI-based credit granting processes.

3.1. – Chapter III, Section 3 AIA provides for a set of obligations placed on all actors across the high-risk AI value chain, namely providers (Articles 16-22), importers (Article 23), distributors (Article 24) and deployers (Article 26). These obligations have a horizontal nature, as they are meant to apply across sectors, but are also complementary inasmuch as their application "should be without prejudice to existing Union law, notably on data protection, consumer protection, fundamental rights, employment, and protection of workers, and product safety". [58]

More specifically, every high-risk AI system shall be designed and developed: (*i*) on the basis of training, validation and testing data sets that meets the quality standards set by Article 10 AIA; (*ii*) to ensure sufficient operative transparency thus enabling deployers to interpret the system's output and use it appropriately; [59] (*iii*) to allow for effective human oversight over their use in order to minimise the risks to fundamental rights pursuant to Article 14 AIA; (*iv*) to achieve an appropriate level of accuracy, robustness, and cybersecurity, and consistently perform throughout its lifecycle. [60] Providers of high-risk AI systems shall ensure (and prove upon request of a national competent authority) that their high-risk AI systems are compliant with these requirements or otherwise immediately take any necessary corrective action to withdraw, disable or recall the AI system. [61]

In addition, for each high-risk AI system providers shall: (*i*) affix the CE marking; [62] (*ii*) register it in the EU database for high-risk AI systems listed in Annex III set up and maintained by the Commission; [63] (*iii*) draw up a declaration of conformity and keep it at the disposal of the national competent authorities for 10 years after its placing on the market or put into service. [64]

Against this background, the AIA expressly addresses regulatory overlaps stemming from the obligations set on providers and deployers that are financial institutions subject to requirements regarding internal governance, arrangements or processes established pursuant to the relevant Union financial services legislation. [65]

---

[57] Recital 64 AIA.

[58] Recital 9 AIA.

[59] Article 13 AIA.

[60] Article 15 AIA.

[61] Articles 16 and 20 AIA.

[62] Pursuant to Article 48 AIA and Article 30(3) Reg. (EC) No 765/2008 by affixing the CE marking the provider indicates that he takes responsibility for the conformity of the AI system with all applicable requirements set out in the relevant Union harmonisation legislation providing for its affixing.

[63] Articles 49 and 71 AIA.

[64] Pursuant to Article 47 AIA, the content of the declaration of conformity is regulated by Annex V and includes, for example, the identification of the provider, a statement of conformity of the AI system with the AIA and, where personal data processed, with the GDPR as well.

[65] Recital 158 AIA.

ISSN 2421-2563

First, at the governance level, the AIA states that competent authorities as defined in Regulation (EU) No 575/2013 (CRR), CCD, MCD, Directives 2009/138/EC (Solvency II), 2013/36/EU (CRD) and 2016/97/EU (IDD) should be preferably designated by Member States as Market Surveillance Authorities (MSAs) for the purpose of supervising the implementation of the AIA with regard to AI systems provided or used by regulated and supervised financial institutions in direct connection with the provision of those financial services. [66]

Secondly, to further enhance regulatory consistency and avoid duplications, the AIA provides for several derogations concerning obligations for providers of high-risk AI systems that are regulated financial institutions. [67] For example, providers of high-risk AI systems are generally required to put in place a quality management system documented through written policies, procedures and instructions at least including the aspects mentioned in Article 17 AIA. However, for providers that are credit or financial institutions this obligation is deemed to be mostly fulfilled by complying with the internal governance rules set by the relevant Union financial law. More specifically, providers of high-risk AI systems are only required to integrate in their existing internal governance setup: (*i*) a risk management system regulated by Article 9 AIA; [68] (*ii*) a post-market monitoring system regulated by Article 72 AIA; and (*iii*) a function for the reporting of serious incidents pursuant to Article 73 AIA. [69]

Similarly, unlike other providers of high-risk AI systems, financial institutions are allowed to keep both the logs automatically generated [70] and the technical documentation [71] required under Articles 10 and 18 AIA as part of the documentation kept under the relevant Union financial services legislation. [72]

Lastly, providers of AI systems intended for credit scoring or assessment purposes, prior to its placing on the market, shall also follow a conformity assessment procedure that does not involve a notified body but that is part of their internal controls. [73]

A similar set of derogations also applies to deployers of high-risk AI systems that are credit or financial institutions.

Generally, deployers are required to take all the appropriate technical and organisational measures to ensure they use high-risk AI systems in accordance with their instructions of use and that the natural persons assigned to ensure human oversight of the high-risk AI systems have the necessary competence, training and authority. Deployers are also required to monitor the operation of the high-risk AI system on the basis of the instructions of use and when relevant, inform providers.

However, for deployers that are credit or financial institutions this monitoring obligation is deemed to be

---

[66] Under the AIA, Member States are still allowed to identify different national authorities but only "in appropriate circumstances, and provided that coordination is ensured". Article 74(6) and Recital 158 AIA.

[67] Originally, Article 9(9) of the 2021 AIA Proposal (COM(2021) 206 final) derogated the risk monitoring duties only with regard to providers that were credit institutions regulated by Directive 2013/36/EU. This led legal scholars to envisage possible regulatory disparities among commercial banks and, for example, investment firms. See AMMANNATI-GRECO, *Piattaforme digitali, algoritmi e Big Data: il caso del credit scoring*, in AMMANNATI-CANEPA-GRECO-MINNECI, *Algoritmi, Big Data, Piattaforme digitali*, Giappichelli, 2021, 193.

[68] Pursuant to Article 9(2) AIA "[t]he risk management system shall be understood as a continuous iterative process planned and run throughout the entire lifecycle of a high-risk AI system, requiring regular systematic review and updating" and aimed at identify risks and adopt appropriate risk management measures.

[69] Article 17(4) AIA.

[70] Articles 18(2) and 19(2) AIA.

[71] Articles 12 and 19 AIA.

[72] This is true, where applicable, also for deployers that are financial institutions. See Article 26(6) AIA.

[73] Article 43 and Annex VI AIA.

ISSN 2421-2563

fulfilled by complying with the rules on internal governance arrangements, processes and mechanisms pursuant to the relevant financial service legislation.

Furthermore, banking entities deploying a high-risk AI system intended for credit scoring or CWA purposes are specifically required to perform, prior to its deployment, a fundamental rights impact assessment (FRIA) of the AI system. However, if deployers are already required to carry out a data protection impact assessment (DPIA) pursuant to either Article 35 GDPR or Article 27 of Directive (EU) 2016/680 both these impact assessments shall be carried out in conjunction and by using also the information provided under Article 13 AIA. Indeed, some of the information included in the FRIA overlap with aspects already covered by the DPIA (e.g. with regard to the description of the categories of natural persons likely to be affected by the AI system and the specific risks posed in their regard). Hence, in order to avoid any additional and unnecessary burden on deployers, the FRIA will ultimately be integrated into the DPIA. To this end, the AI Office will develop a questionnaire template that deployers will be able to use to meet this obligations. [74]

Ultimately, the overarching objective of these derogations is to partially integrate providers' and deployers' procedural obligations into similar obligations and procedures the already existing under the CRD and, more limitedly, under the GDPR, CCD and MCD.

These legislative approach, although positively aimed at minimizing administrative burdens for financial institutions, will pose significant challenges in both designating national MSAs and actually carrying out market surveillance tasks under the AIA.

First, the integration of AIA obligations into the existing CRD framework may pose significant challenges in setting up and performing efficient market surveillance. Indeed, while the risk management and internal governance set up implemented under the CRD responds to the overall objective of ensuring the safety and soundness of credit institutions, the quality and risk management obligations provided by the AIA are instrumental in reaching the overarching goal of protecting health, safety and fundamental rights of persons that could potentially be affected by abusive AI systems.

This inherent, prevailing, prudential nature is true also for other Union financial legal acts potentially overlapping with the AIA, such as the Capital Requirements Regulation (n. 575/2013/EU, CRR), but also for other level two Guidelines, such as those on internal governance. [75]

Furthermore, as mentioned, even CCD and MCD provisions are currently not focused on ensuring that credit-granting decisions consider consumers' best interests: [76] only under the CCD2 creditors will be explicitly required to take into account consumers' overall indebtedness while assessing their creditworthiness.

However, the integration of obligations aimed at protecting fundamental rights into a governance and risk management framework designed to ensure financial stability will blur the line between conduct and prudential supervision over financial institutions. For example, as pointed out by the ECB, [77] while the SREP has an *ex post* and prudential set-up, the AI conformity assessment is part of an *ex ante* internal control carried out

[74] Recital 96 and Article 27 AIA.

[75] EUROPEAN BANKING AUTHORITY, *Guidelines on internal governance under Directive 2013/36/EU* (luglio 2021, EBA/GL/2021/05).

[76] The EC Final Report on "Study on possible impacts of a revision of the CCD", published in May 2021, pointed out that the Directive does not include specific obligations to ensure that consumer credit is devised and marketed to consumers in their best interest. In this regard, one of the issues is that Article 8(1) of the CCD "does not establish whether the assessment should be creditor-focus (i.e. risk assessment) or borrower-focused (i.e. affordability assessment), a dichotomy which according to some scholars, is a sign that creditworthiness are not necessarily carried out in the best interests of the consumer".

[77] Opinion of the ECB of 29 December 2021 on a proposal for a regulation laying down harmonised rules on artificial intelligence (CON/2021/40).

ISSN 2421-2563

by the provider to evaluate elements that might not be prudential in nature. Also, although the ECB does not plan on taking on any role as MSA,[78] the AIA clarifies that national MSAs supervising credit institutions regulated under the CRD should timely report to the ECB any information of potential interest for prudential supervision.[79] Therefore, at the implementation stage, what will play a pivotal role in actually reducing duplications and administrative burdens for the industry will be the ability of designated MSAs to effectively exchange information and cooperate at both national and Union level.[80]

Moreover, the AIA does not expressly address all potential overlaps stemming from the obligations therein set on providers and deployers that are financial institutions. For instance, pursuant to Article 15 AIA, high-risk AI systems shall be designed and developed in such a way that they achieve an appropriate level of accuracy, robustness (e.g. through technical redundancy solutions, including backup or fail-safe plans), and cybersecurity. Also, as mentioned, pursuant to Articles 13(1) and 14(1) AIA, high-risk AI systems shall allow for human oversight and shall be transparent for deployers. However, it remains to be assessed if and to what extent financial institutions are already required to ensure similar standards under other legal acts such as, *inter alia*, the Regulation on digital operational resilience for the financial sector (DORA, e.g. Article 6)[81] and the Regulatory Technical Standards on ICT risk management framework (e.g. Articles 21 and 23).

3.2. – With specific regard to automated credit-granting processes, another level of regulatory complexity stems from the partially overlapping scope of application of the individual right to an explanation set by Articles 22 GDPR, 18 CCD2 and 86 AIA.[82]

Namely, pursuant to Recital 171 and Article 86 AIA natural persons affected by decisions based mainly upon the output of a high-risk AI system should have the right to obtain from the deployer clear and meaningful explanations if such decisions produce legal effects or similarly significantly and adversely affect their health, safety and fundamental rights. Such explanation shall convey a description of the role of the AI system in the decision-making procedure and the main elements of the decision taken.

Furthermore, like Recital 71 GDPR, Recital 58 AIA recognizes that credit scoring and creditworthiness assessment practices significantly affect fundamental rights of natural persons "since they determine those persons' access to financial resources or essential services such as housing, electricity, and telecommunication services".[83]

This provision extensively overlaps with the rights enshrined in Articles 13(2)(f), 14(2)(g), 15(1)(h) and 22 GDPR[84] as well as in Article 18(8)(a) CCD2. Indeed, as mentioned, both the CCD2 and the GDPR ad-

[78] Ibid.

[79] Article 74(7) AIA.

[80] Pursuant to Article 70(2) AIA, Member States shall communicate to the Commission the identity of the notifying authorities and the market surveillance authorities and the tasks of those authorities by 2 August 2025.

[81] Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011.

[82] GAGGERO-VALENZA, *Le nuove prassi valutative del merito creditizio tra GDPR, CCD II e AI Act-New Creditworthiness assessment practices between GDPR, CCD II and the AI Act*, in *European Journal of Privacy Law & Technologies*, 1 (2024).

[83] Also, Recital 171 AIA stresses that the "explanation should be a clear and meaningful and should provide a basis on which the affected persons are able to exercise their rights".

[84] For an Italian comment see VALENZA, *Modelli innovativi di valutazione del merito creditizio: contesto normativo e prospettive di regolamentazione*, in PROTO (ed.), *Umano e non umano nelle relazioni tra intermediari e clienti*, Pacini Giuridica, 2024, 107. For an ex-

ISSN 2421-2563

dress automated decision-making processes affecting natural persons by providing for consumers/data subjects right to obtain human intervention, to express their view and to obtain an explanation of the automated decision. [85]

However, while Article 18 CCD2 and Article 86 AIA respectively refer to creditworthiness assessments and decisions that "involve the use of automated data processing" or are "mainly based" on automated outputs, the wording of Article 22 GDPR only refers to "solely" automated decisions. As mentioned, the EUCJ in the Schufa's judgment nonetheless excluded a formalistic approach by clarifying that Article 22 GDPR also applies to credit decisions that draw strongly on the automated score even if the final decision formally rests with a third human party. Hence, the GDPR, the CCD2 and the AIA convey a similar explainability standard: the right to obtain clear, comprehensible and meaningful information on the logic, the risks, the significance, the effects, the functioning and the main elements (i.e. the main parameters and their respective weight) of the automated decision-making process.

Incidentally, it is worth noticing that the EUCJ's stance on the Schufa case was based on the assumption that a formal interpretation of Article 22 GDPR would deprived data subjects of their right to obtain an explanation, to contest and to obtain a review of a credit-decision took on the basis of an automated credit score or CWA. [86]

Therefore, this interpretative approach could change once the AIA and the CCD2 apply and provide affected persons with similar rights irrespective of how strongly the decision draws on the automated output.

The AIA expressly addresses this regulatory overlap by clarifying its residual nature. Namely, Article 86(3) AIA states that it only applies if the right therein enshrined is not already recognized under other Union legal acts. Hence, it can be inferred that in cases of AI systems intended for credit scoring or CWA purposes, Article 86 AIA would not apply unless the affected natural person does not qualify as either a data subject under the GDPR or a consumer under the CCD2. Indeed, Article 86 AIA appears to have a wider scope of subjective application inasmuch as it covers automated CWA or credit scoring practices affecting natural persons not qualifying as consumers and irrespective of whether the AI systems processed personal data.

With regard to the CCD2-GDPR interplay, Recital 30 CCD2 clarifies that it leaves unprejudiced the GDPR "which applies to any processing of personal data carried out by creditors and credit intermediaries falling within the scope of the CCD2". Hence, by setting a stricter general prohibition of solely automated decisions Article 22 GDPR should prevail and apply, unless the creditor provides statistical and empirical evidence proving that the credit decision is not *de facto* solely or strongly based on the automated output. [87]

---

tra-EU comment on the regulatory proposal see, for example, VEALE-BORGESIUS, *Demystifying the Draft EU Artificial Intelligence Act*, in *Computer Law Review International*, 4, 2021, 104; SMUHA-AHMED-RENGERSB-HARKENS-MACLAREN-PISELLI-YEUNGG, *How the EU Can Achieve Legally Trustworthy AI: A Response to the European Proposal for an Artificial Intelligence Act*, Elsevier, August 2021, 54.

[85] Recital 71 GDPR.

[86] Opinion of the Advocate General, § 48; EUCJ, Judgement of 7 December 2023, Case C-634/21, §63-64.

[87] Such a burden of proof could be met, for example, where the creditor provides evidence that a loan was granted, in similar circumstances, despite a negative credit score or, on the opposite, that a credit application was refused on similar grounds in multiple cases notwithstanding the positive credit score assigned. Indeed, a similar standard of proof is required to prove the ancillary nature of insurance policies vis-à-vis the conclusion of a consumer credit contract. Namely, according to the Banking and Financial Ombudsman (ABF)'s case law, even when the insurance policy is defined as optional in the contract, it shall be assumed to be compulsory (and therefore included in the calculation of the annual percentage rate (APR)), when: (a) it is a credit insurance policy; (b) the policy and the loan agreement are signed at the same time and have the same duration; and (c) the insurance indemnity is linked to the residual debt. However, the intermediary may provide proof to the contrary, for instance by producing other personal loan contracts granted without an insurance policy to different customers with the same creditworthiness as the complainant and under conditions similar to those of the loan under examination. See, for example, ABF decision n. 23718/2020 (available in Italian). More gen-

ISSN 2421-2563

If such proof is not provided, a CWA could be lawfully drawn from an automated credit score only if (a) authorized by law and (b) based on a lawfulness basis pursuant to Articles 22(2)(b) and 6(1) GDPR. More specifically, as clarified in the Schufa judgement, credit decisions based on automated processing of personal data would be exceptionally allowed under Article 22(2)(b) GDPR if Article 18 CCD2 qualifies as a law authorizing it. Should this be the case, private credit information agencies could then invoke the lawfulness basis of the pursuit of a legitimate interest to carry out automated CWAs (by also proving that there aren't any data friendlier ways to perform their tasks). On their part, banks and other financial companies could also invoke the lawfulness basis of the compliance with a legal obligation since they are required by law to carry out a creditworthiness assessment.

Alternatively, Article 18 CCD2 could be regarded as a *lex specialis* derogating the cross-sectoral provision set by Article 22 GDPR. In this case, however, in order to avoid diminishing consumer rights, Articles 13(2)(f), 14(2)(g) and 15(1)(h) GDPR should still apply. Indeed, while the GDPR and the AIA provide for both *ex ante* and *ex post* explanatory duties by requiring creditors to provide clients with information on the AI systems in general but also of the decision reached, the CCD2 wording seems to suggest an information duty *vis-à-vis* consumers that only applies once a creditworthiness assessment has been carried out as it never refers to general information on the functioning of the decision-making procedure before a decision has been reached. Such information would therefore need to be conveyed to consumers as data subjects pursuant to the GDPR since any creditworthiness assessment implies the processing of their personal data. [88]

The problems stemming from the implementation of the right to obtain an explanation of automated credit decisions do not end with the identification of the applicable law. Indeed, even before the adoption of the AIA and the CCD2, the legal debate on the intelligibility of automated decisions gradually shifted from the *an* to the *quomodo* of algorithmic transparency. In this regard, scholars discussed many explanation models, such as: (*i*) the "counterfactual explanation" (consisting in providing data subjects with information about "the smallest change to the world that can be made to obtain a desirable outcome", i.e. the so called "closest possible world" scenario); [89] (*ii*) the "demographic-based" explanation (involving the disclosure of the relevant characteristics the addressee of the automated decision shares with other people who received a similar automated outcome); [90] (*iii*) the "performance-based" explanation (through which data subjects are informed about the percentage of people sharing their characteristic that received an erroneous automated outcome). [91]

It is beyond the scope of this article to discuss the details of each solution and their ability to meet the transparency threshold set by the GDPR, [92] it is however of pivotal importance to stress that despite these

---

erally, for an overview of the Ombudsman's case law see the Abdriged version of the Annual Report available in English at https://www.arbitrobancariofinanziario.it/abf/relazione-annuale/index.html.

[88] Like Articles 13(2)(f), 14(2)(g) and 15(1)(h) GDPR, Article 26(11) AIA provides for "deployers of high-risk AI systems referred to in Annex III that make decisions or assist in making decisions related to natural persons shall inform the natural persons that they are subject to the use of the high-risk AI system."

[89] S. WACHTER-B. MITTELSTADT-C. RUSSELL, *Counterfactual Explanations without Opening the Black Box: Automated Decisions and the GDPR*, in 31 *Harvard Journal of Law & Technology* 2 25, 2018.

[90] M. HILDEBRANDT, *The Dawn of a Critical Transparency Right for the Profiling Era*, in J. BUS-M. CROMPTON-M. HILDEBRANDT-G. METAKIDES (eds), *Digital Enlightenment Yearbook* 2012 (IOS Press 2012) 49. See also A. MANTELERO, *Personal data for decisional purposes in the age of analytics: From an individual to a collective dimension of data protection*, in 32 *Computer Law & Security* 238, 2016; L. KAMMOURIEH *et al.*, *Group Privacy in the Age of Big Data*, in L. TAYLOR-L. FLORIDI-B. SLOOT (eds.), *Group Privacy. New Challenges of Data Technologies*, in *Philosophical Studies Series*, Vol. 126, Springer, 2017, 43.

[91] L. EDWARDS-M. VEALE, *Slave to the Algorithm? Why a 'Right to an Explanation' Is Probably Not the Remedy You Are Looking For*, in 16 *Duke Law & Technology Review* 18 55, 2017.

[92] For further details on this topic see also C. TABARRINI, *Understanding the Big Mind. Does the GDPR Bridge the Human-*

scholarly efforts the issue of what amounts to a "meaningful explanation" of an automated decision still remains unsolved.

In this regard, compared to Recital 71 GDPR, Recital 56 CCD2 makes an additional effort by clarifying that a comprehensible explanation entails a description "of the functioning of the automated processing used, including the main variables, the logic and risks involved".

The reference to the main variables also recalls the wording used by the provisions of the Omnibus Directive [93] and the Platform to Business (P2B) Regulation [94] together known as the "New Deal for Consumers" regulatory package. Indeed, both regulatory acts provide for information duties aimed at informing the weaker part of the B2C/B2P contractual relationship (respectively the consumer and the business) of the main parameters determining the ranking of offers presented on the platform as a result of the search query, as well as the relative importance of those parameters as opposed to other parameters. [95]

Lastly, both the Digital Market and Digital Services Acts reiterated the importance to provide clear, plain, intelligible, user-friendly and unambiguous information on algorithmic decision-making and human review as well as on profiling practices (including, but not limited to, profiling within the meaning of Article 4(4) GDPR) to enable end users to be aware of such practices and facilitate contestability. [96] These provisions therefore add on the ongoing debate by clarifying that an explanation is meaningful inasmuch as it enables the addressee to foresee how their behaviour can influence the automated decision-making process, while not requiring a full disclosure of the algorithmic logic underneath. [97]

Overall, transparency of AI systems generally seems to entail algorithmic predictability conveyed through a reasoned description of the most significant criteria used to reach an automated decision as well as an explanation of how the recipient of such decision can actively influence the outcome with their behaviour. [98] Moreover, as clarified by the EUCJ in the Schufa case, a meaningful explanation of an automated business decision doesn't need to infringe upon IP or trade secret rights. In fact, it doesn't involve algorithms' disclosure, [99] con-

---

Machine Intelligibility Gap?, in *Journal of European Consumer and Market Law*, 9, 4, 2020, 135-143 and ID., *Explainability Due Process: legal guidelines for AI-based business decisions*, in R. SENIGAGLIA-C. IRTI-A. BERNES (eds), *Privacy and Data Protection in Software Development for International Information Society Services*, Springer, 2022.

[93] Directive (EU) 2019/2161 of the European Parliament and of the Council of 27 November 2019 amending Council Directive 93/13/EEC and Directives 98/6/EC, 2005/29/EC and 2011/83/EU of the European Parliament and of the Council as regards the better enforcement and modernisation of Union consumer protection rules.

[94] Regulation (EU) 2019/1150 of the European Parliament and of the Council of 20 June 2019 on promoting fairness and transparency for business users of online intermediation services.

[95] Article 6a Dir. 2011/83/EU as amended by Directive (EU) 2019/2161; Article 5 Reg. 2019/1150/EU.

[96] Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act), Recital 72 and Article 15(1); Regulation (EE) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services and amending Directive 2000/31/EC (Digital Services Act).

[97] For further details on this predictability standard see TABARRINI, *Explainability Due Process: legal guidelines for AI-based business decisions*, in SENIGAGLIA-IRTI-BERNES (eds), *Privacy and Data Protection in Software Development for International Information Society Services*, Springer, 2022.

[98] Recital 24-25 Reg. 2019/1150/EU and Recitals 22 Dir. 2019/2161/EU.

[99] On the applicability of Trade Secret protection to algorithms see M. MAGGIOLINO, *EU Trade Secrets Law and Algorithmic Transparency*, AIDA, Giuffrè, 2018, 211. More generally, on Trade Secret protection see M.A. LEMLEY, *The Surprising Virtues of Treating Trade Secrets as IP Rights*, in 61 *Stanford Law Review* 311, 2008; OTTOLIA, *Il D.Lgs. N. 63/18 di attuazione della Dir. 2016/943/UE sulla protezione dei segreti commerciali fra tutela e bilanciamenti*, in *Nuove leggi civili commentate*, 2019, 5, 1091; D'IPPOLITO, *Il principio di limitazione della finalità del trattamento tra data protection e antitrust. Il caso dell'uso secondario di Big Data*, in *Il diritto dell'informazione e dell'informatica*, 2018, 6, 943; CRESPI, *Commento sub artt. 98-99 c.p.i.*, in VANZETTI (ed.), *Codice proprietà industriale* (Giuffrè 2013) 1101; DE SANCTIS, *I soggetti del diritto d'autore*, II ed., Giuffrè, 2005, 167.

ISSN 2421-2563

trary to what was occasionally argued in past, for example, by Italian courts. [100] Notably, this balance was also reiterated during the drafting process of the AIA by stressing that any disclosure should be limited to "to the minimum necessary information for individuals to exercise their right to an effective remedy and to the necessary transparency towards supervision and enforcement authorities." [101]

4. – In light of the above, AI development, testing and ongoing monitoring need to be carefully designed and implemented to detect and correct bias, algorithmic opacity, accountability gaps and, more generally, infringements of all relevant legislatives act. This results in the multiplication of compliance burdens on the industry, especially for providers and deployers that are already subject to stringent regulations such as financial institutions carrying out AI-based CWAs. [102]

For example, under the AIA, data quality and bias detection safeguards will need to be thoroughly documented via the FRIA, as part of the DPIA. [103] At the same time, the internal prudential risk management and governance setup will need to be integrated with risk monitoring and reporting functions focused on AI-related risks to fundamental rights of clients. This will include, for example, documenting and monitoring AI explainability standards applied to automated CWAs. [104] Similarly, AI human oversight will require providers and deployers' staff to be numerically sufficient and adequately skilled and trained. Moreover, to comply with their customer information and protection duties, credit institutions developing or deploying AI systems for CWAs purpose could be required to integrate their current paperwork with AI-related information both at the pre-contractual and contractual stage, as well as to setup ongoing review processes of automated decisions contested by clients.

As mentioned, AI conformity assessments can be carried out by AI provider based on their 'internal control', which, in turn, could reflect harmonised European standards.

---

[100] For example, in a case concerning the denial opposed by the Italian Ministry for Education, University and Research (MIUR) to a teacher's labor union's request to access the source code underpinning the software used to take entirely automated decisions regarding the trans-regional transfer of school staff, the Italian Administrative Regional Tribunals (TAR) granted access to the source code as the algorithmic description provided by the software company was found insufficient. TAR subdivision III-bis, judgement n. 3769/2017.

[101] Proposal For A Regulation Of The European Parliament And Of The Council Laying Down Harmonised Rules On Artificial Intelligence (Artificial Intelligence Act) And Amending Certain Union Legislative Acts, Brussels, 21.4.2021, Com(2021) 206 Final, §3.5.

[102] D'ALOIA, *Il diritto verso il nuovo mondo. Le sfide dell'Intelligenza Artificiale*, in *BioLaw Journal Law – Rivista di BioDiritto*, n. 1, 2019, 3 ss.; AMIDEI, *Intelligenza Artificiale e diritti della persona: le frontiere del "transumanesimo"*, in E. GABRIELLI-RUFFOLO (a cura di), *Intelligenza Artificiale e diritto*, in *Giur. It.*, luglio 2019, 1658 ss.; CELOTTO, *Come regolare gli algoritmi. Il difficile bilanciamento fra scienza, etica e diritto*, in AGE, n. 1, 2019, 47 ss.; S. LANNI, *Dataquake: intelligenza artificiale e discriminazione del consumatore*, in *Nuovo Diritto Civile*, n. 2, 2020, 97 ss.; SCIASCIA, *Reputazione e potere: il social scoring tra distopia e realtà, in Giornale di diritto amministrativo*, n. 3, 1 maggio 2021, 317.

[103] The principle of non-discrimination is affirmed in Article 21 of the EU Charter of Fundamental Rights.

[104] Algorithmic accountability refers to the responsibility of entities to ensure fairness, transparency and non-discrimination in AI models. Regarding accountability, see S. KELLEY-A. OVCHINNIKOV, *Anti-discrimination Laws, AI, and Gender Bias: A Case Study*, in *Non-mortgage Fintech Lending*, September 27, 2021, abstract available at the link: ssrn.com/abstract=3719577. On the importance of explainability and how to make credit scoring predictions more transparent and justifiable: M. BÜCKER-G. SZEPANNEK-A. GOSIEWSKA-P. BIECEK, *Transparency, auditability, and explainability of machine learning models in credit scoring*, in *Journal of the Operational Research Society*, 2021; X. DASTILE-T. CELIK, *Making Deep Learning-Based Predictions for Credit Scoring Explainable*, in *IEEE Access*, vol. 9, 2021, 50426 ss.; N. KOZODOIA-J. JACOBA-S. LESSMANN, *Fairness in credit scoring: Assessment, implementation and profit implications*, in *European Journal of Operational Research*, 297 (2022), 2021, 1083 ss.

ISSN 2421-2563

To this end, on 22 May 2023 the European Commission issued a Standardisation request [105] in support of Union policy on AI to the European Committee for Standardisation (CEN) and the European Committee for Electrotechnical Standardisation (CENELEC), requesting harmonised European standards on ten new technical areas [106] linked to the AIA requirements for 'high-risk AI systems' to be covered in conformity assessments and quality management systems. These standards are expected to be delivered by 30 April 2025 and will therefore potentially address many auditing challenges of automated CWA models.

4.1. – According to Article 23 CCD, national law must provide effective, proportionate, and dissuasive sanctions for violation of provisions on consumer CWA. Member States are therefore allowed to set the penalty they deem preferable as long as it complies with these standards.

This margin of discretion has however led to interpretative uncertainties under the CCD, recently addressed also by the EUCJ. Indeed, on 11 January 2024 the EUCJ decided a case C-755/22 concerning whether CCD allows for a national law to penalize a creditor where failure to fulfil its obligation to examine a consumer's creditworthiness has not resulted in any harmful consequences for the consumer. More specifically, in the case at hand the national law provided for the credit agreement to be void and for interests to be forfeited.

As mentioned, the CCD does not currently make any express reference to consumers' best interests when regulating CWAs. However, in its settled case-law, the EUCJ has stressed that the obligation to examine the consumer's creditworthiness contributes to ensuring high and equivalent levels of consumer protection across the EU. [107] Hence, in deciding case C-755/22, the Court reaffirmed that the objective of Article 8 CCD is also to protect individual customers from the risk of over-indebtedness, which can occur even if the debt has been repaid and after a long period has elapsed. Therefore, the EUCJ found the nullity of the contract compliant with Article 23 CCD even when applied to agreements fully performed by both parties and when consumers did not suffer any harmful consequences as a result of creditors failure to carry out a proper CWA. [108]

---

[105] See *Commission Implementing Decision on a standardisation request to the European Committee for Standardisation and the European Committee for Electrotechnical Standardisation in support of Union policy on artificial intelligence*, 22 May 2023, C(2023)3215, available at the link: https://ec.europa.eu/transparency/documents-register/detail?ref=C(2023)3215&lang=en.

[106] 1. Risk management system for AI systems; 2. Governance and quality of datasets used to build AI systems; 3. Record keeping -built-in logging capabilities in AI systems; 4. Transparency and information to the users of AI systems; 5. Human oversight of AI systems; 6. Accuracy specifications for AI systems; 7. Robustness specifications for AI systems; 8. Cybersecurity specifications for AI systems; 9. Quality management system for providers of AI system; 10. Conformity assessment for AI systems.

[107] See EUCJ judgments of 27 March 2014, LCL Le Crédit Lyonnais, C-565/12, EU:C:2014:190, § 42, and of 5 March 2020, OPR-Finance, C-679/18, EU:C:2020:167, § 21.

[108] Judgment of the Court (Third Chamber) of 11 January 2024 (request for a preliminary ruling from the Okresní soud Praha-západ – Czech Republic) – Nárokuj s.r.o. v EC Financial Services, a.s. Available at the link: http://data.europa.eu/eli/C/2024/1513/oj. Aluigi, Osservatorio europeo – Sull'obbligo di verifica del merito creditizio dei consumatori, in I Contratti, n. 2, 1 marzo 2024, 225. It is worth mentioning that the EUCJ judgment concerned a provision of Czech law, while Italian regulations do not nullify a contract in similar cases. In Italy there are provisions for prudential supervisory sanctions and, in case of proven harmful consequences, compensation that can be claimed through civil proceedings where damages occured. Nevertheless, the judgment in question is of particular importance also for Italian entities because it reflects the EUCJ's attention to compliance with obligations to assess the creditworthiness of consumers. See Request for a preliminary ruling of 2 February 2024, Bankinter Consumer Finance (Spain), Case C-88/24. For an analysis of the Italian Banking regulatory framework on creditworthiness assessments see, for example, Dolmetta, *Merito del credito e concessione abusiva*. Dopo Cass. n. 1810/2021, in DB – Dialoghi di diritto dell'economia, ottobre 2021; De Chiara, *Verifica del merito creditizio*, in *Commentario al Testo unico delle leggi in materia bancaria e creditizia*, diretto da Capriglione, con la collaborazione di Pellegrini, Sepe e V. Troiano, t. III, Padova, 2012, 1869; Franchi, *Il ruolo del merito creditizio nella rinnovata disciplina in tema di composizione della crisi da sovraindebitamento: la chiusura di un cerchio?*, in *Riv. dir. banc.*, 2021,

ISSN 2421-2563

This topic is however undoubtedly destined to raise further discussions, especially in the context of the use of AI systems for CWA purposes under both the AIA and the new CCD2 provision on CWA. [109]

Indeed, as discussed above, it is currently not clear which regulatory regime will apply to automated CWA given the overlapping obligations set by the AIA, the GDPR and the CCD2. In turns, this raises the question of which penalty regime should apply. For example, should Article 18 CCD2 take precedence over the application of Article 86 AIA, consumers could potentially be precluded from lodging a complaint before the relevant MSA if they have grounds to believe that a violation of their explanation rights under the AIA occurred. [110] In this case, they could however potentially invoke the application of the national penalty provided for infringements of Article 18 CCD2, if the violation concerns the information provided by the creditor after a credit decision has been reached. Indeed, as mentioned, Article 18 CCD2 does not seem to provide for *ex ante* information duties concerning the use of AI systems for CWA purposes. However, consumers could still enjoy *ex ante* information rights pursuant to Articles 13(2)(f), 14(2)(g) and 15(1)(h) GDPR. Therefore, consumers affected by automated CWAs having grounds to believe that creditors violated their obligations to provide them with information on the use of AI systems before carrying out the CWA could not invoke a violation of Article 18 CCD2 but only of the GDPR.

Moreover, depending on the applicable law Member States will have to allocate market surveillance and financial oversight tasks. It remains to be seen, for instance, which national authority (or authorities) will be designated in each Member State as MSA under the AIA and which will especially be tasked with market surveillance over AI systems intended to be used for CWA purposes. [111] This in turn, will determine the type of powers, corrective measures and sanctions that creditors could face when developing or deploying automated CWAs.

4.2. – As stressed in Draghi Report, [112] ensuring full regulatory compliance across the EU is of pivotal importance to prevent another notorious obstacle to European competitiveness: gold-plating. This is even more crucial in relation to Union laws subject to the Brussel Effect, such as the AIA. Indeed, credit information agencies or creditors developing in-house AI-based scoring tools qualify as providers pursuant to Article 3(3) AIA, irrespective of their location inasmuch as their AI system is commercialized in the EU or the credit score produced is anyway used in the EU. Hence, for example, a US-based credit information agency

---

501 ss.; ADDANTE, *La sostenibilità del credito immobiliare fra meritevolezza del consumatore e responsabilità del creditore*, in *Giust. civ.*, 2022, 925 ss. MINNECI, *La verifica del merito creditizio: una valutazione a sua volta insindacabile?*, in *Riv. trim. dir. econ.*, Suppl. n. 2 al n. 3, 2021, 354; MATTASSOGLIO, *La valutazione "innovativa" del merito creditizio del consumatore e le sfide per il regolatore*, in *Dir. banc. merc. fin.*, 2020, 187 ss., spec. 200; ID., *Innovazione tecnologica e valutazione del merito creditizio del consumatore*, Milano, 2018; RABITTI, *Credit scoring via machine learning e prestito responsabile*, in *Riv. dir. banc.*, 2023, 175.

[109] This assumption is further corroborated by the fact that, not even a month after the C-755/22 judgement was issued, the topic was brought again at the attention of the EUCJ by a Spanish court which asks for EUCJ's interpretive opinion arguing that the administrative penalties provided for by national laws for creditors violating their obligation to assess consumers' creditworthiness, to date, are purely theoretical and ineffective. Therefore, the referring court asks the EUCJ whether national laws should expressly provide effective and dissuasive civil penalties.

[110] Article 85 AIA.

[111] Pursuant to Article 70(2) AIA, Member States will have to make such decision by 2 August 2025.

[112] The future of European competitiveness, Part B – In-depth analysis and recommendations, September 2024, 319-320 available at https://commission.europa.eu/document/download/ec1409c1-d4b4-4882-8bdd-3519f86bbb92_en?filename=The%20future%20of%20European%20competitiveness_%20In-depth%20analysis%20and%20recommendations_0.pdf.

producing credit scores outsourced and used by a bank established in the EU would qualify as a provider pursuant to the AIA. [113] Similarly, a bank established in the EU carrying out creditworthiness assessments via outsourced AI-based tools or based on outsourced credit scores would qualify as a deployer within the meaning of Article 3(4) AIA irrespective of whether the provider of the AI systems or the credit score is located in or outside the Union. [114]

As mentioned, however, to reach the goal of ensuring legislative coherence, avoid duplications and ensure full regulatory compliance, many operative challenge will need to be faced by both authorities and businesses adopting AI-based creditworthiness procedures. Indeed, providers and deployers that are financial institutions will be simultaneously subject to multiple legislative acts, such as: *i*) the CRR/CRD and the EBA GLs on internal governance for internal and model governance requirements; *ii*) the GDPR, especially with regard to automated processing of consumers' personal data; *iii*) the CCD/CCD2/MCD, with respect to consumers' CWAs involving automated data processing; and the *iv*) the AIA, with respect to the risk management, internal governance and explainability standards of high-risk AI systems.

Looking ahead, other important regulatory interplay may concern the revision of the MCD and the new FIDAR (Financial Data Access Regulation). [115]

On the one hand, on December 2021 the EC sent to the EBA a call for advice regarding the MCD review. In that occasion, the EBA pointed out that the EC should consider addressing AI-related risks potentially posed to consumer protection (e.g. risk of financial exclusion and discrimination) in the AIA as a sector-specific regulation. Since the CCD2 now regulates these aspects, it is very likely that the recast MCD will also include more detailed provisions to this effect and, in this scenario, it will be essential that during the review process utmost attention is given to the maximum alignment with the existing legislation, primarily with the CCD2 and the AIA.

On the other hand, FiDAR establishes a framework of rules for the access, use, and sharing of certain categories of customer data held by financial entities (so-called data holders), with the goal of promoting digital transformation and accelerating the adoption of new business models in the European financial sector. [116] Therefore, FiDAR will inevitably partially overlap with the GDPR especially with regard to customer protection provisions (e.g. permission dashboards to be used by consumers to monitor and manage their consent and the potential financial exclusions' risks stemming from data subjects refusing consent). [117] To this end,

[113] Recital 21, AIA.

[114] Indeed, Recital 22 AIA clarifies that "[t]o prevent the circumvention of this Regulation and to ensure an effective protection of natural persons located in the Union, this Regulation should also apply to providers and deployers of AI systems that are established in a third country, to the extent the output produced by those systems is intended to be used in the Union". For the previous version of the recital see Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain Union legislative acts – Analysis of the final compromise text with a view to agreement, 5662/24, Brussels, 26 January 2024, recital 6a.

[115] Proposal for a regulation of the European Parliament and of the Council on a framework for Financial Data Access and amending Regulations (EU) No 1093/2010, (EU) No 1094/2010, (EU) No 1095/2010 and (EU) 2022/2554 (COM (2023) 360). To date, it is expected the approval of the compromise text by the EU Council and the start of the trilogue negotiations among Commission, Council and Parliament.

[116] As for its scope of application, the FIDAr proposal aims to cover all financial data with potential added value (including anything related to mortgages and loans) to provide consumers with personalised financial products and services aligned with their needs.

[117] Although data related to life, health and sickness insurance products or collected in the context of a consumer's creditworthiness assessment are excluded from the scope of the FiDAR, there could still be distortive effects and risks of financial exclusion if a customer that refuses consent to share data is exposed to risk of obtaining a negative creditworthiness assessment and, therefore, be refused access to credit. To avoid the risk of misuse, the FIDAr proposal seeks to ensure that customers' refusal to consent to share sets of their data shall not constitute legitimate ground for creditors to refuse them access to financial products.

ISSN 2421-2563

according to the FIDAr proposal, the EBA shall develop Guidelines in close cooperation with the European Data Protection Board to clarify how data therein covered can be used for consumer CWA building on the existing CCD, MCD and LOGL framework.

Additionally, irrespective of which provision applies, many operative challenges remain. For example, it still remains to be determine how creditors developing or deploying AI systems for CWAs could satisfy the explainability standard set by the AIA, the CCD2 and the GDPR. This issue is especially since, irrespective of the technology used, the CCD does not determine either the manner in which the creditor must discharge the CWA obligation nor the obligations imposed on it in relation to the result of the evaluation. [118] Creditors are always allowed to legitimately refuse credit in the exercise of their entrepreneurial autonomy. However, the already existing obligation for creditors to act in good faith and motivate the refusal will now need to take into account the algorithmic transparency standards set in this regard by the CCD2, the AIA and the GDPR when AI systems are involved in the CWA.

Therefore, despite the declared objective of the AIA is to minimize burdens, both MSA and credit institution will face many changes and challenges while ensuring compliance with an overlapping and multi-layered regulatory framework.

From a legislative standpoint, an approach to mitigate the problem of regulatory overlaps could be to implement a streamlining of all the relevant laws, applying a principle of speciality to favour a limited application of cross-sectoral or Level 2 legal acts. For example, as illustrated above in para. 2.3, the recast Level 1 text contained in the CCD2 is more detailed than the current LOGL text. Hence, LOGL's provisions on consumer protection features of the CWAs (including those related to the use of tech-enabled processes) appear less detailed than the Level 1 text, thus potentially resulting to be duplicative, potentially restrictive and at times inconsistent with the recast CCD's intent and pre-requirements.

For this reason, removing CWAs carried out under the CCD2 from the scope of the LOGL might seem a solution to effectively overcome inconsistencies and overlapping of text between Level 1 and LOGL wording. However, this would also imply that all other LOGL provisions related to the monitoring part do no longer apply to credit products under the recast CCD.

Alternatively, another regulatory approach could be to exclude credit products covered under the recast CCD from the creditworthiness assessment requirements outlined in the LOGL. This solution would preserve the applicability of the LOGL to the originating and monitoring stages of the credit lifecycle, while eliminating contradictions or overlap between Level 1 and Level 3 texts.

Another option could be to maintain unchanged the current scope of application of the LOGL while expunging any reference to tech-enabled credit granting processes. This would minimize changes to the current regulatory regime, while also avoiding the risk of overlaps and duplications with regard to AI-enabled credit-granting processes.

From a governance and surveillance perspective, cross-sectoral cooperation and guidance will definitely be the key. Indeed, from the feedback submitted by stakeholders to the targeted consultation on AI in the financial sectors recently closed by the EC [119] it is evident that there is a strong general preference for cross-

[118] Judgment of the Court (Third Chamber) of 11 January 2024 (request for a preliminary ruling from the Okresní soud Praha-západ – Czech Republic) – Nárokuj s.r.o. v EC Financial Services, a.s., §32. See also, to that effect, EUCJ judgment of 18 December 2014, CA Consumer Finance, C-449/13, EU:C:2014:2464, § 36), or judgment of 6 June 2019, Schyns, C-58/18, EU:C:2019:467, §§ 42 and 43.

[119] Documents related to the targeted consultation on artificial intelligence in the financial sector are available at https://finance.ec.europa.eu/regulation-and-supervision/consultations-0/targeted-consultation-artificial-intelligence-financial-sector_en.

ISSN 2421-2563

sectoral guidance (where applicable) and sectoral oversight convergence towards financial surveillance authorities (where possible). Against this background, in this first AIA implementing stage, a pivotal role will be played by the newly established DG-Connect AI Office. However, given the highly complex governance and surveillance setup created by the AIA, the AI office will need support by both European Surveillance Authorities and national financial authorities to properly address regulatory overlaps in every market sector and issuing cross-sectoral guidance inasmuch as possible.

AI is penetrating every market sector with disruptive implications that will affect the way both businesses and surveillance authorities currently carry out their tasks. This, in turn, is increasingly creating demand of new interdisciplinary skills and calls for technology and law to find common ground. In this context, effective customer protection across the EU will depend on the ability of all stakeholders involved to cooperate at both national and Union level to create new expertise able to align what is technologically feasible to what is ethically and legally admissible to keep the internal market human-centric.

ISSN 2421-2563