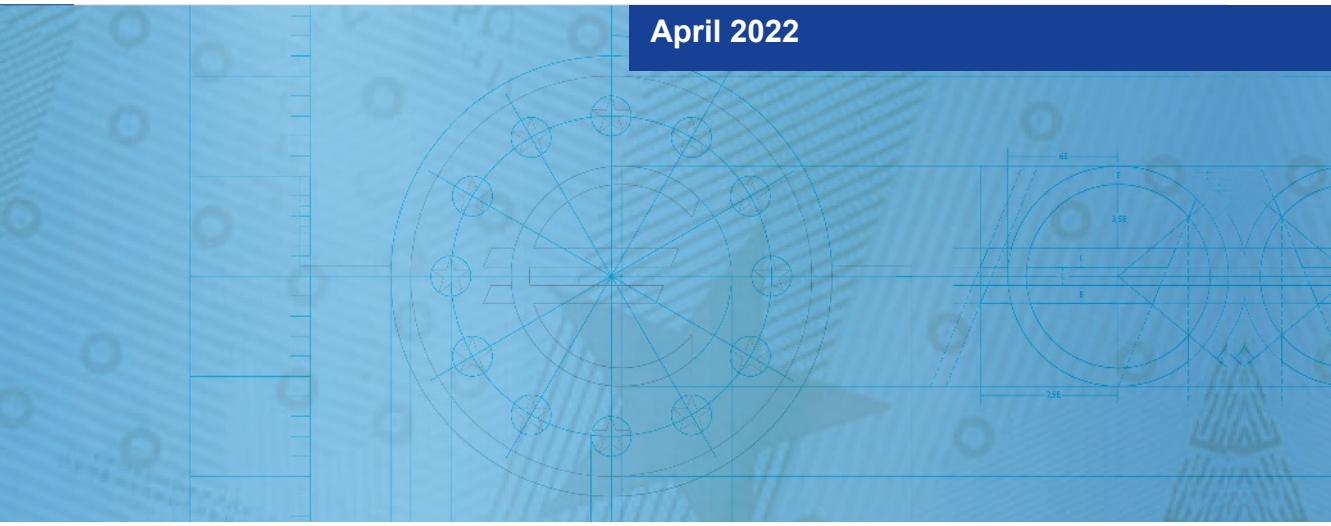
EUROPEAN CENTRAL BANK

EUROSYSTEM

Continuity and change – how the challenges of today prepare the ground for tomorrow

ECB Legal Conference 2021



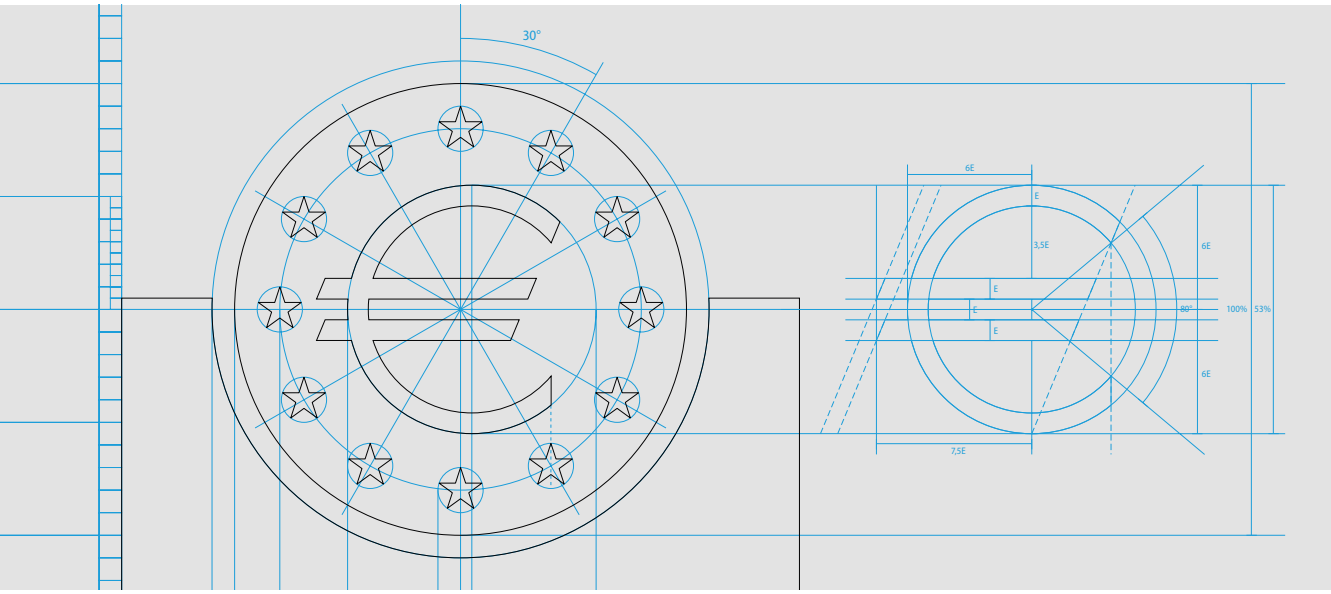
April 2022

EUROPEAN CENTRAL BANK

EUROSYSTEM

Continuity and change – how the challenges of today prepare the ground for tomorrow

ECB Legal Conference 2021



Postal address 60640 Frankfurt am Main, Germany
Telephone +49 69 1344 0
Website www.ecb.europa.eu

Neither the European Central Bank nor any person acting on behalf of the Bank is responsible for the use that might be made of the following information.

The content of the articles, including but not limited to the accuracy of references to bibliography, legislation and court cases, is the sole responsibility of the authors. The views expressed in the articles exclusively represent the authors' own opinions and do not necessarily reflect those of the ECB. Reproduction and translation for non-commercial purposes are authorised, provided the source is acknowledged.

Luxembourg: Publications Office of the European Union, 2022

PDF	ISBN 978-92-899-4990-3	ISSN 2467-0057	doi:10.2866/255752	QB-BX-22-001-EN-N
Print	ISBN 978-92-899-4989-7	ISSN 2467-0049	doi:10.2866/04525	QB-BX-22-001-EN-C

© European Central Bank, 2022

For any use or reproduction of photos or other material that is not under the copyright of the European Central Bank, permission must be sought directly from the copyright holders.

Contents

Introduction
By Chiara Zilioli* 7

Change and continuity in law – Keynote speech
By Christine Lagarde* 13

PART I

Introduction of the President of the European Court of Justice
By Christine Lagarde* 23

Proportionality as a matrix principle promoting the effectiveness of EU law and the legitimacy of EU action – Keynote speech
By Koen Lenaerts* 27

Symposium on proportionality

Legal Symposium on proportionality
By Chiara Zilioli* 45

Proportionality in German constitutional law
By Dieter Grimm* 48

The EU law principle of proportionality and judicial review: its origin, development, dissemination and the lessons to be learnt from the Court of Justice of the European Union
By Diana-Urania Galetta* 55

Proportionality review in economic governance: a manifestation of the formal rationality of modern law?
By Tomi Tuominen* 77

Proportionality and discretion in EU law: in search of clarity
By Vasiliki Kosta* 94

Proportionality in comparative perspective in view of the *PSPP/Weiss* saga
By Iddo Porat* 108

How the Council applies the principle of proportionality when legislating
By Thérèse Blanchet* 128

PART II

When you need change to preserve continuity: climate emergency and the role of law
By Frank Elderson* 141

Panel 1: Dialogue between courts: what is the future for legal pluralism?

On the dialogue between courts: what is the future for legal pluralism?
By Frank Elderson 151

Legal pluralism in context
By Ineta Ziemele* 155

Constitutional pluralism and the principles of counterpoint law
By Miguel Poiares Maduro* 162

Dialogue between courts: what is the future for legal pluralism? A view from the Court of Justice of the European Union
By Juliane Kokott and Christoph Sobotta 168

A better alternative to legal pluralism: *e pluribus unum*
By Daniel Calleja Crespo and Tim Maxian Rusche* 177

Panel 2: Rule of law: what is the fate of the rule of law in the EU?

Rule of law: what is the fate of the rule of law in the European Union?
By Edouard Fernandez-Bollo* 191

How the European rule of law can support democratic transitions: on the criminal responsibility of biased judges
By Armin von Bogdandy and Luke Dimitrios Spieker* 197

The CJEU and the normalisation of the rule of law crisis
By Renáta Uitz* 211

What is the fate of the rule of law in the EU?
By Laura Codruța Kövesi* 224

Panel 3: Relationship between law and markets

On the relationship between law and markets
By Isabel Schnabel* 231

Lending, liquidity and the law
By Katharina Pistor* 237

Reconsidering the EU's economic ideas on markets and law: towards greater effectiveness, accountability and democracy
By Vivien A. Schmidt* 262

Deconstitutionalising the Economic and Monetary Union
By Marco Dani* 282

Law and the markets – the role of international financial institutions between market participants and public policy: a practitioner's view
By Barbara Balke* 309

Panel 4: Digitalisation of finance: the challenges from a central bank and supervisory perspective

Digital finance: emerging risks and policy responses
By Fabio Panetta* 321

The EU Digital Finance Strategy – regulatory challenges and legal approaches
By Jan Ceyssens* 328

Central bank digital currency: Caribbean pathways
By Diana Wilson Patrick* and Thandiwe Lyle* 340

AI credit scoring and evaluation of creditworthiness – a test case for the EU proposal for an AI Act
By Katja Langenbucher* 362

Panel 5: The COVID-19 crisis: a Hamiltonian moment for Europe?

The COVID-19 crisis: a Hamiltonian moment for Europe
By Frank Smets* 391

The innovative European response to COVID-19: decline of differentiated integration and reinvention of cohesion policy
By Bruno De Witte* 394

Fiscal surveillance and coordination in post-pandemic times – between uncertainty and opportunity
By Paul Dermine* 403

Post-COVID-19 E(M)U interinstitutional balance: assessment and outlook
By Diane Fromage* 421

The COVID-19 crisis – a Hamiltonian moment for Europe?
By Rhoda Weeks-Brown* 436

Concluding synopsis
By Chiara Zilioli* 451

Programme of the ECB Legal Conference 2021 **459**

Biographies **467**

AI credit scoring and evaluation of creditworthiness – a test case for the EU proposal for an AI Act

By Katja Langenbucher*

On 21 April 2021, the European Commission published a proposal for a regulation laying down harmonised rules on artificial intelligence (hereinafter the "proposal").[1071] In the spirit of fostering innovation and at the same time ensuring the trustworthiness of artificial intelligence (AI) applications, the proposal follows a risk-based approach. Under this framework, many AI systems face no or minimal obligations. By contrast, those which are considered "high risk" must comply with newly established requirements. A few AI applications are entirely prohibited.

Among the high-risk categories we find "AI systems to be used to evaluate the creditworthiness of natural persons or establish their credit score".[1072] This goes back to the concern that they "may lead to discrimination of persons or groups and perpetuate historical patterns of discrimination … or create new forms of discriminatory impacts".[1073] The ensuing compliance requirements concern the quality of data sets, technical documentation, human oversight and more.

This paper provides a brief overview on algorithmic credit scoring and the evaluation of creditworthiness, introduces the proposal's risk-based approach and critically discusses its compliance requirements and institutional design. It makes two contributions to the debate. First, it challenges the proposed regulatory architecture which risks a dual standard between bank supervisors and AI supervisors. Second, it highlights the normative, not quantitative nature of fundamental rights,

* Goethe University and Leibniz Institute SAFE, Frankfurt a. M.; affiliated faculty at SciencesPo, Paris; visiting faculty at Fordham Law School, NYC; project leader at ZEVEDI, Hessen. This paper has profited enormously from feedback during the following events: 2nd AI & Policy Events, ETH Zürich; 3rd Edinburgh Fintech Law Lecture; 6th Luxemburg FinTech Conference; Frankfurt Institute for the history of banking; Frankfurt ConTrust Center; FinCoNet Seminar on creditworthiness assessments; Fordham Law School's Seminar on Privacy and Technology Law; Hamburg Network on AI and Law; Helsinki & Edinburgh's Digital Capital Markets Conference; Mannheim ZEW and MaCCI; NYU's Privacy Research Group. My heartfelt thanks go to the wonderful colleagues who invited me to speak and to all participants in the discussion. Special thanks go to Talia Gillis, Columbia Law School, for many rounds of cross-Atlantic discussion.

1071 Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act), Commission (2021a). In what follows, references to articles and recitals for which no source is given are from this proposal.

1072 Annex III (5)(b).

1073 Recital 37.

concluding that these are ill-suited as a benchmark for banking and credit scoring supervision.

1 Algorithmic credit scoring and evaluation of creditworthiness: a brief overview

Historically, loan decisions were based on a mix of qualitative and quantitative information. Where individual loan officers decided on the creditworthiness of each applicant, cognitive errors and implicit biases often distorted the assessment of credit default risks. The introduction of statistical computations in the 1950s greatly enhanced the understanding of risk and was quickly introduced in both banks and – where available – credit scoring agencies.[1074] Currently, most established credit scoring agencies use a fixed number of input variables such as, for instance, free income or past credit history, to produce standardised scores.

With the advent of big data, powerful computing power and machine learning technology, novel forms of credit scoring have surfaced.[1075] In addition to (or instead of) a limited number of variables, they collect "alternative data" such as web browsing or purchasing patterns, the location of the applicant's computer, Facebook friends, typos in text messages, tastes in music, font types found on electronic devices, time needed to fill out an application, or diligence in charging one's smartphone.[1076] The relevant score is established based on correlations between such data and historical data on, for instance, timely repayment or ability to pay high interest on a short-term loan.[1077]

Machine learning models of this type can contribute to better pricing of credit decisions based on more traditional variables. It might also help (re-) evaluate existing credit portfolios. Additionally, it has raised high hopes for the unbanked, underbanked, or credit invisible. Applicants who do not have the credit history to inform the traditional factors may profit from alternative data to achieve a better score. Banks, especially those with a FinTech bent, might be willing to broaden their creditworthiness assessments, thereby accessing new markets. The use of algorithms might reduce the extent of discrimination when compared to a world in which humans make all the decisions.[1078]

[1074] Lauer (2017).

[1075] Adolff and Langenbucher (2020); Burrell and Fourcade (2021). See Pistor (2020) on the predictive power of data.

[1076] Bruckner (2018). On the anonymity of such data and privacy concerns see Boenisch (2021).

[1077] Aggarwal (2021); Barocas and Selbst (2016); Bruckner (2018); for an evaluation of the predictive accuracy of models using email usage and psychometric variables see Djeundje et al. (2021).

[1078] Such is the finding of Rambachan et al. (2021).

However, a growing body of research suggests that not all loan applicants will profit to the same extent.[1079] Predictions based on machine learning depend on training data. The quality of their predictions is only as good as the match between how the training data describes the world and the world as it is. If the training data reflects past inequality, any applicant who shares features with a historically underserved group will be flagged as less creditworthy than a comparable applicant who does not share the relevant feature. Historic bias of this kind has been understood to present a troublesome concern[1080], and has motivated the EU proposal to qualify AI credit scoring systems and credit evaluation systems as high risk.

Some of these concerns go back to modelling bias.[1081] Because input to a model is shaped by data (or lack of data), conditional expectation functions look different across various groups. Some underbanked will profit if their alternative data profile resembles the profile of candidates which in the past have been successful at getting loans (e.g. the new immigrant who lacks the specifics of a national credit history but has a steady income, is male and in early middle age). For underbanked candidates with an alternative data profile which does not match historically successful candidates, AI scoring is not necessarily as helpful and might even backfire (e.g. the candidate might just about make a traditional score, but the AI score might be lower due to gender, race, religion, age, educational background etc.).

In some instances, the problem can be mitigated, for example by defining output variables (e.g. 35% of the successful candidates must be female) or by fitting separate models for each group. This latter approach faces complex questions as to whether anti-discrimination law prohibits using data on protected group membership for the purposes of credit risk model building.[1082] On a side note, as to this specific question, the EU proposal takes a bold step forward: “To the extent that it is strictly necessary for the purposes of ensuring bias monitoring, detection, and correction in relation to high-risk AI systems, the providers of such systems may process special categories of data (referred to in Article 9 General Data Protection Regulation [GDPR][1083], Article 10 Law Enforcement Directive[1084], Article 10 Data

---

1079 Burrell and Fourcade (2021). See for a case study on upstart: Langenbucher and Corcoran (2021); for the use of credit scores in car insurance pricing: Kiviat (2019a); on the use of credit reports by employers: Kiviat (2019b); for personalised transactions more generally: Wagner and Eidenmüller (2019).

1080 Barocas and Selbst (2016); Graham (2021); Gillis (2020).

1081 Blattner and Nelson (2021), p. 12 et seq.

1082 ibid.

1083 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (OJ L 119, 4.5.2016, p. 1).

1084 Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA (OJ L 119, 4.5.2016, p. 89).

Protection Regulation for EU Institutions[1085]) subject to appropriate safeguards for the fundamental rights and freedoms of natural persons …".[1086]

However, there are more worries. Modelling bias is compounded if the training data used for machine learning systems is less rich for protected classes. The model will then favour some variables and not adequately cope with others ("majority bias").[1087] Additional concerns go back to data bias.[1088] It is a typical feature of the underbanked to have a "thin" credit file with low explanatory power as to the underlying credit report data.[1089] The way in which default is reported may not adequately reflect relevant details of the default situation or the observables may be less informative. The risk of discrimination along those lines and the potential distrust of consumers when faced with AI seem to have motivated the Commission to list AI credit scoring as a high-risk AI system.

2 The proposal: a brief overview

2.1 What is an "AI system"?

The proposal applies to "AI systems". These are defined as "software that is developed with one or more of the techniques and approaches listed in Annex I [of the proposal] and can, for a given set of human-defined objectives, generate outputs such as content, predictions, recommendations, or decisions influencing the environments they interact with".[1090] As to the techniques mentioned in this definition, Annex I, which is rather comprehensive, lists three approaches, namely machine learning, logic- and knowledge-based approaches, and statistical approaches.[1091]

2.2 The top-down, risk-based approach

The proposal is organised top-down, establishing "common normative standards for all high-risk AI systems".[1092] This distinguishes the proposal from sectoral approaches which treat AI systems differently according to their intended area of use in, for instance, health, air traffic, or finance.[1093]

1085 Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ L 295, 21.11.2018, p. 39).

1086 Article 10(5). For a critique, see EDPB-EDPS (2021).

1087 ibid.

1088 ibid.

1089 ibid.

1090 Article 3(1).

1091 Spindler (2021).

1092 Recital 13.

1093 Comparing sectoral and omnibus approaches to privacy in credit scoring, see Langenbucher (2020); for AI more generally, see Hacker (2021).

In preparatory work the EU has considered sectoral approaches as one regulatory option. However, rather than addressing broad sectors (such as finance or health), the approach was framed as "ad hoc… or revision of existing legislation on a case-by-case basis".[1094] Against that background, the Commission was understandably concerned about "sectoral market fragmentation" and an increased "risk of inconsistency".[1095] Broader framing of sectors might have mitigated this concern.

Eager to avoid overregulation, the proposal has introduced a risk-based approach. Legal rules are tailored to "the intensity and the scope of the risks that AI systems can generate".[1096] A small number of AI applications are entirely ruled out, such as, for instance, social scoring if done by public authorities or on their behalf.[1097] Many applications face only minimal or no compliance requirements. Between these categories we find high risk applications.

2.3 AI systems where conformity assessment procedures exist

Some AI systems are intended to be used as safety components of a product or are products themselves. They are automatically considered high risk if they are required to undergo third party conformity assessments according to a list in Annex II of the proposal. This Annex captures products as diverse as toys, lifts, cableway installations and medical devices.

Conformity assessments are for those AI systems integrated into the EU New Legislative Framework. This (general) framework for product regulation imposes the duty to run conformity assessments on the producer of a product (rather than on a public agency). Private standard-making bodies develop guidance on how to assess conformity. Compliance with such guidance leads to a presumption of conformity with the proposal's requirements.[1098] This presumption does not extend to conformity with other legal rules such as, for instance, the GDPR.[1099]

For AI systems that operate in an area where conformity assessment procedures exist, standard-setting bodies such as the European Committee for Standardisation (CEN) will be important rule-setters.[1100] Consequently, there is concern regarding lobbying and regulatory capture.[1101]

[1094] Commission (2021b), p. 43, referencing the NYC Council proposal for a regulation on automated hiring tools.
[1095] ibid., p. 45. For a positive view on the sectoral approach, see Spindler (2021).
[1096] Recital 14.
[1097] Recital 17, Article 5(1)(c).
[1098] Article 40.
[1099] EDPB-EDPS (2021) recommends that compliance with the GDPR should be a precondition of assessing conformity under the proposal.
[1100] On the interplay between the proposal and these rules, see Spindler (2021).
[1101] Veale and Zuderveen Borgesius (2021).

2.4 Stand-alone AI systems

AI systems where no conformity assessment procedures exist are held to a different standard. Relevant risks in these areas are (exclusively) harm to health, safety, or fundamental rights. Put differently: AI systems are considered high risk if they "have a significant harmful impact on the health, safety and fundamental rights of persons".[1102] Annex III specifies a list of areas of use for these stand-alone AI systems. The critical areas listed encompass: (1) biometric identification, (2) critical infrastructure, (3) education, (4) employment, (5) essential private services, (6) law enforcement, (7) migration, and (8) administration of justice and democratic processes.

The Commission has the power to update Annex III, but it may not add new areas.[1103] Updating requires showing why the relevant context belongs to one of the existing areas.[1104] Additionally, the Commission would need to establish that the relevant risk is, "in respect of severity and probability of occurrence, equivalent or greater than the risk of harm or adverse impact posed by the high-risk AI system already referred to in Annex III".[1105] The drafters include a long list of considerations to be balanced when making this decision, such as, for instance, the intended purpose of the AI system, the extent of its use, harm already caused, the scale and extent of such harm, any imbalances in power between the user of the AI system and the adversely impacted person, and the degree of protection provided by existing EU law.[1106]

3 AI credit scoring and evaluation of creditworthiness as a high-risk system

Machine learning models used for credit decisions fall under Annex III No 5 if they concern natural[1107] persons. Annex III No 5 captures access to essential public and private services. Among the private services listed, two qualify: systems which establish priority in accessing emergency services[1108] and systems which are "intended to be used to evaluate the creditworthiness of natural persons or establish their credit score".[1109]

[1102] Recital 27: the "and" should probably be read as "or"; the text of Article 7(1)(b) is more precise.
[1103] Article 7(1); critique in EDPB-EDPS (2021): "black-and-white effect".
[1104] Article 7(1)(a).
[1105] Article 7(1)(b).
[1106] Article 7(2).
[1107] Annex III No 5(b). AI systems used for internal rating of legal persons are not covered under the Annex.
[1108] Annex III No 5(c).
[1109] Annex III No 5(b).

3.1 Essential private services

The proposal does not specify what makes a service "essential". Recital 37 lists three examples, namely "housing, electricity and telecommunication services". Any AI system which evaluates creditworthiness in the context of these three services will be considered high risk. Additionally, recital 37 refers to "access to financial resources". A narrow reading would suggest that only loan contracts give such access. By contrast, a broader reading might understand any firm that lets the consumer pay in instalments as giving "access to financial resources". This could cover any mail order firm which offers a "buy now, pay later" service and uses AI to evaluate its customers' creditworthiness. Whether such a firm qualifies as high risk would then depend on a follow-up question: is "access to financial resources", which is mentioned only in recital 37 but not in the Annex, automatically an "essential private service"? Or are we looking at a two-prong test where we need access to financial services which must be given in the context of an essential private service? The latter reading would suggest that some mail order firms could qualify, but not others. Similarly, bank products which involve an assessment of creditworthiness but are not a loan, for instance investment opportunities or an insurance offer, might qualify as an essential service – or not.

3.2 Relevant risks and the spirit of product regulation

Recital 37 explains the risk the drafters have in mind for AI scoring systems: "they determine those persons' access to financial resources … AI systems used for this purpose may lead to discrimination of persons or groups and perpetuate historical patterns of discrimination… or create new forms of discriminatory impacts".

Considering the discussion above about historic modelling and data bias[1110], this might not come as a surprise. However, against the background of the intense global discussion on algorithmic fairness, the nonchalance of the proposal is surprising. From a legal perspective the question of when exactly "persons or groups" are being discriminated against is equally hotly debated as that of what historic bias entails. Economists have repeatedly pointed out that statistical discrimination is a necessary feature of creditworthiness evaluations and financial institutions insist on it as a form of protecting business.

The proposal does not address this question but claims that they are dealt with in other parts of EU law (such as the GDPR and anti-discrimination directives).[1111] Instead, it brings product regulation to mind. The drafters frame AI systems as dangerous products in need of quality management.[1112] Their "ingredients" (software and data)[1113] have to be

[1110] See Section 1.
[1111] On implications for tort law see Grützmacher (2021).
[1112] Articles 9 and 17.
[1113] Article 10.

monitored, tested and documented.[1114] Manuals have to be prepared for users,[1115] and a human overseer must make sure everything goes according to plan.[1116] Where risk management systems are already a requirement of the law, carve-outs apply.[1117]

This spirit of regulating a "dangerous product" shapes what type of compliance the drafters expect as to quality and risk management. The proposal (roughly) distinguishes five categories, which focus on data and data governance, technical documentation and record-keeping, transparency, human oversight and, lastly, robustness, accuracy, and cybersecurity. Requirements are adapted to the situation of (professional) developers and users. There are no rules on end consumers in the proposal.

3.3 Quality of data sets

I have said above that the quality of predictions produced by an AI system depends on its training data.[1118] Improving the quality of data sets, as required by Article 10, serves that end. Training, validation and testing data sets "shall be subject to appropriate data governance".[1119] Some hints are given as to what might count as "appropriate", but the term remains vague. The drafters seem to hope that data can be "relevant, representative, free of errors and complete"[1120], and that its statistical properties, once again, have to be "appropriate".[1121]

"Sloppy data" are often a root cause for algorithmic discrimination[1122], aggravated by the fact that alternative data are not as carefully scrutinised as, for instance, credit reporting data.[1123] The proposal mentions "data collection" as a space where data governance and management practices are in order.[1124] It reminds developers to assess "availability, quantity and suitability of the data sets"[1125] and to identify "data gaps or shortcomings".[1126]

Additionally, the drafters call for an "examination in view of possible biases"[1127]: whether they have model construction or data gathering (or

---

[1114] Articles 11, 12 and 15.
[1115] Article 13.
[1116] Article 14.
[1117] See Section 4 below for credit institutions.
[1118] See Section 1 above.
[1119] Article 10(2).
[1120] Article 10(3).
[1121] Article 10(3).
[1122] Barocas and Selbst (2017).
[1123] See for the EU, the GDPR and national law (for instance section 31 of the German Federal Data Protection Act [BDSG]); for a US comparison see the Fair Credit Reporting Act.
[1124] Article 10(2)(b).
[1125] Article 10(2)(e).
[1126] Article 10(2)(g).
[1127] Article 10(2)(f).

both) in mind is not clear. As noted above, the proposal opens the door to the mitigation of model risks by allowing for the possibility to fit a model to specific groups, if to do so is "strictly necessary for the purposes of ensuring bias monitoring, detection and correction"; processing of especially sensitive data under the GDPR is allowed.[1128]

3.4 Transparency

Article 13 addresses transparency and the provision of information to "users". In a credit scoring context, one might expect potential borrowers to qualify as "users", able to profit from guidance on what the scoring process entails and how they might adapt their behaviour to better their score.[1129] However, "users" under the proposal are only those entities or persons which employ the AI system.[1130] These are, for instance, banks, mobile phone companies or credit scoring agencies, not the private citizens who are being scored. As noted in the proposal, the GDPR is more relevant for these private citizens being scored, which the drafters of the proposal understand as complementary to it.[1131]

However, meaningful access and transparency for borrowers is more difficult to realise under the GDPR than one might assume.[1132] Article 6(1) of the GDPR allows for processing of data as soon as the data subject has consented. Such consent will often be included in general terms and conditions if banks score their own customers, based on data to be gathered on where, when, and how customers use their payment cards or make wire transfers. More complicated issues as to consent under the GDPR arise if scoring agencies use alternative data from the internet. If consent is given in a social media context, the wording of the general terms and conditions might be broad enough to capture credit scoring. If this is not the case, consent will often be requested as part of the process when signing up for a credit platform.[1133] While this consent most likely satisfies the legal requirement (i.e. the letter of the law), it is more doubtful as to whether it also satisfies the spirit of the law. Research by computer scientists has long discussed how "uninformed consent" can be triggered by certain properties of the graphical user interface such as the position of the notice, the type of choice offered and the content framing.[1134] The more giving consent resembles a "tick-the-box" exercise, the more it loses its significance as an initial threshold under the GDPR.[1135]

1128 Article 10(5). See Section 1 above.
1129 On "gaming the system" in this context, see Langenbucher (2020), p. 541 et seq.
1130 Article 3(4).
1131 EU Commission (2021a), Explanatory Memorandum, p. 4.
1132 Langenbucher (2020).
1133 Alternatively, Article 6(1)(b) GDPR allows for processing at the request of the data subject to prepare entering into a contract, Article 6(1)(f) permits data processing if it is necessary for "the purposes of the legitimate interests pursued by the controller", see Langenbucher (2020).
1134 Utz et al. (2019).
1135 Pistor (2020); Comparative law exercise at Langhanke (2018).

As to transparency and explainability, the GDPR seems even less helpful. While Article 13 of the GDPR regulates access to one's data, which includes information about the "purposes of processing"[1136], the drafters clearly did not have the explanation of a credit score or the reasons for denial of credit in mind. Credit risk models are carefully guarded trade secrets, a fact the GDPR explicitly acknowledges and counts as a reason to limit access to one's data.[1137] Refusal of a credit contract is mentioned in the GDPR, but exclusively in the context of an automated action.[1138] Neither the explainability of scoring nor the evaluation of creditworthiness are the focus of this recital. Rather, it is restricted to purely automated decision-making.[1139] Along those same lines, Article 13(2)(f) of the GDPR requires "meaningful information about the logic involved" only where automated decision-making is at stake. Even then, it is unclear whether the concept of giving "meaningful information" and addressing the "logic involved" is up to the challenge of data being processed via algorithms which, possibly, not even their user can explain. Additionally, the GDPR's top-down, omnibus approach seems to focus more on access as such (a paradigmatic case being access to one's own medical data), rather than explaining to the data subject the intricacies of what their data is used for.

The more variables enter into the computation of a score, the more unlikely it is that the data subject's rights flowing from Articles 6 and 13 of the GDPR provide an adequate remedy. To understand which data was used, the data subject might need to keep a file on websites visited and check their data privacy rules, which is an unrealistic prospect.[1140]

Seen from this angle, credit scoring already falls between the cracks of the GDPR's regulatory framework.[1141] The proposal deepens these concerns by relegating borrowers under the GDPR (which doesn't always help them) and not granting them an enforceable right to an explanation for the collection and use of their data.

Coming back to the "users" that Article 13 of the proposal has in mind, the spirit is again one of product regulation. The drafters focus on who will employ the AI system and try to make sure they understand the system's output well enough. Paragraph 2 requires instructions for use and paragraph 3 specifies what these should provide for. At the same time, full transparency, for instance of credit risk models, does not seem to be intended. In vague terms, the proposal stipulates that operation of the system must be "sufficiently" transparent and that the "type and degree of transparency" must be "appropriate". Given that the reason for qualifying AI

1136 Article 13(1)(c) of the GDPR.
1137 Recital 63.
1138 Recital 71 of the GDPR.
1139 Langenbucher (2020).
1140 But see the judgment of the European Court of Justice on burden of proof as to active consent: Case C-61/19, *Orange Romania* EU:C:2020:901; in the context of debt management: Oberlandesgericht Naumburg of 10.3.2021 – 5 U 182/20.
1141 See for a comparison to the United States Langenbucher (2020); more generally: Hacker (2021); for damages under the GDPR: *Bundesverfassungsgericht* (2021); Landgericht Lüneburg (2021); Paal and Aliprandi (2021).

credit scoring as high risk lies with the risk it entails for fundamental rights, one might expect detailed transparency on a potential risk of disparate impact. Yet, Article 13(3)(b)(iv) speaks only of "performance as regards the persons or groups… on which the system is intended to be used". "Performance" is defined as "the ability of an AI system to achieve its intended purpose".[1142] The "intended purpose", as defined by the proposal[1143], is what the provider had in mind when developing the AI system. However, what the provider of an AI credit scoring software has in mind, is a prediction of credit default risk, not of the impact of the AI credit scoring software on fundamental rights. Somewhat lamely, recital 47 reminds us that "instructions of use" are to "include concise and clear information, including in relation to possible risks to fundamental rights and discrimination". But the recital immediately adds: "where appropriate". Applied to credit scoring and evaluation of creditworthiness, there is little reason to assume that the drafters had transparency as to the inner workings of credit risk models in mind.

3.5 Human oversight

Human oversight has often been thought to provide evidence of trustworthiness or dignity to private citizens faced with automated decision-making by AI.[1144] The proposal has a different role in store for human oversight, in line with its product regulation and quality management approach. Human oversight is not intended to serve the consumer, process input or to provide explanations. Instead, Article 14 requires high risk systems "to be designed and developed in such a way… that they can be effectively overseen by natural persons".[1145] The human overseer is envisaged as someone able to "interrupt the system through a 'stop' button",[1146] to "correctly interpret the high-risk AI system's output"[1147] and to "disregard, override or reverse the output".[1148] In contrast to transparency requirements, the drafters explicitly expect the "human-in-the-loop" to prevent or minimise "risks to… fundamental rights".[1149]

In some situations, human oversight of this type will be very useful. Examples include, for instance, the use of AI in internal compliance or risk management to provide "red flags" based on key words. Where such key words are used in compliance management, they will often require a second pair of human eyes to understand their significance and possibly supervise and retrain the AI. Without a second look of this type, AI will increase costs, rather than lowering them, hence there is a business case for a human-in-the-loop. It is less clear whether, in terms of consumer

[1142] Article 3(18).
[1143] Article 3(12).
[1144] EDPB-EDPS (2021); Veale and Zuiderveen Borgesius (2021).
[1145] Article 14(1).
[1146] Article 14(4).
[1147] Article 14(4)(c).
[1148] Article 14(4)(d).
[1149] Article 14(2).

credit, there will necessarily be a business case along those lines. Relevant concerns include the amount of the credit, the extent to which it was automated and the cost of a human-in-the-loop when compared to an automatic refusal of credit.

The problem seems even more intricate if the human overseer is not (only) supposed to evaluate a "red flag", but to consider the entire credit evaluation/scoring suggested by the machine. The hope for a smarter-than-the-machine human overseer might be an unrealistic one. Empirical studies suggest that people are unable to perform oversight functions of this type, mostly because they are bad at judging the quality of AI predictions which can lead to discounting accurate AI results.[1150] Instead, cognitive errors and biases might find a back door via the human oversight doublecheck.[1151] Additionally, there is a worry that all concerned parties fall under the spell of a false sense of security which ends up diminishing both accountability and incentives to enhance the quality of the AI system.[1152] "Automation bias", the phenomenon of deferring to an AI's recommendation which has been highlighted by computer scientists and psychologists, is explicitly taken up by the proposal.[1153] Faced with this phenomenon, users are encouraged to train their personnel and highlight this risk. The chances of producing a meaningful[1154] second look, rather than a rubber-stamping exercise, will often be slim.[1155]

4 Regulatory architecture: the special regime for credit institutions

The proposal contains carve-outs from its decision to follow a top-down, omnibus approach rather than a sectoral approach. Where conformity assessment procedures exist, the proposal's requirements are integrated into these procedures.[1156] Against the background of existing heavy regulation of credit institutions, exemptions have been accommodated for internal risk management and for market supervision.

[1150] Green and Chen (2019); Green (2021).
[1151] FRA (2020): "Humans overrule … mainly when the result from the algorithm is not in line with their stereotypes"; Green and Chen (2019).
[1152] Green and Chen (2019); Green (2021); Koulu (2020).
[1153] Article 14(4)(b); Green and Chen (2019); Green (2021).
[1154] While some regulators have started asking for "meaningful" human intervention (see Green and Chen (2019); Green (2021)), the proposal does not include such a qualifier.
[1155] For the additional concern that end consumers have no right to access the service provided without the use of an AI system, see Spindler (2021).
[1156] See Section 2.3 above.

4.1 Internal risk management

A first element of a sectoral, rather than an omnibus regulatory approach concerns internal risk management of credit institutions.[1157] The proposal has integrated its conformity assessment as well as some of the obligations regarding risk management, post marketing monitoring and documentation into the existing framework under the Capital Requirements Directive 2013 (CRD IV).[1158, 1159]

Article 74 of CRD IV stipulates the basic duties of financial institutions to have robust internal governance arrangements. This includes a clear organisational structure, consistent lines of responsibility, processes to identify risk, and adequate internal control mechanisms. The European Banking Authority (EBA) issues guidelines on relevant processes.[1160]

Following up on Article 74 of CRD IV, the proposal understands high-risk AI management to be part of the general CRD IV risk management procedures.[1161] Identifying and analysing known and foreseeable risks associated with the AI systems would be integrated in the financial institution's regular risk assessment procedures. Reasonably foreseeable misuse is to be estimated and evaluated, post-marketing monitoring being put in place.[1162] Appropriate risk management measures must be identified through testing.[1163] Any residual risk must be judged acceptable, considering the purpose of the AI system, including reasonably foreseeable misuse.[1164] Technical documentation and automatically generated logs must be maintained as part of the documentation required under Article 74 of CRD IV.[1165]

Going one step further along those same lines, a credit institution that is in compliance with Article 74 of CRD IV is deemed to fulfil the proposal's requirement to put a quality management system in place.[1166] This includes regulatory compliance, testing the AI design, technical standards, systems and procedures for data management, post-market monitoring, record-keeping, accountability and more.[1167] The same is true for monitoring obligations if a credit institution is not the provider, but instead the user of

---

1157 Credit institutions are defined in Article 4(1)(1) of the Capital Requirements Regulation (CRR), Regulation (EU) No 575/2013 of the European Parliament and of the Council of 26 June 2013 on prudential requirements for credit institutions and investment firms and amending Regulation (EU) No 648/2012 (OJ L 176, 27.6.2013, p. 1).

1158 Directive 2013/36/EU of the European Parliament and of the Council of 26 June 2013 on access to the activity of credit institutions and the prudential supervision of credit institutions and investment firms, amending Directive 2002/87/EC and repealing Directives 2006/48/EC and 2006/49/EC (OJ L 176, 27.6.2013, p. 338).

1159 Recital 80.

1160 Article 74(2) of CRD IV.

1161 Article 9(9).

1162 Article 9(2).

1163 Article 9(5) to (7).

1164 Article 9(4).

1165 Articles 18 and 20, and Article 29(5).

1166 Article 17(3).

1167 See in detail Article 17(1); for post-market monitoring see Article 61(4).

an AI system.[1168] As far as the provider's quality management obligations and the user's monitoring duties are concerned, the proposal additionally suggests "limited derogations"[1169] to avoid regulatory overlap. A special regime applies to the reporting of serious incidents. If a credit institution is a provider and regulated under CRD IV, only a malfunction that constitutes a breach of obligations under EU law must be reported to market surveillance authorities.[1170]

4.2 Supervisory authorities and enforcement

The second sectoral, rather than omnibus element in the proposal's regulatory architecture concerns supervision. Chapter 3 of the proposal stipulates that, as a rule, the regulatory framework of the EU Regulation on Market Surveillance and Compliance of Products[1171] shall apply to AI systems. However, as far as credit institutions are concerned, the competent authority, which may be the European Central Bank[1172] will be the market supervisor under financial services legislation.[1173] The hope is to ensure "coherent enforcement"[1174], given that AI is not only used in customer-facing applications, but also in internal risk-management, in governance, in trading and more.

Banking supervisory agencies face the need to define how they will go about filling this new role. The proposal expects them to take over (yet more) market surveillance activities.[1175] The conformity assessment, which providers of high-risk AI systems have to undergo prior to placing the product on the market, will be integrated for credit institutions in the supervisory review and evaluation process (SREP) under CRD IV.[1176] Against that background, the proposal grants supervisors "full access to the training, validation and testing datasets"[1177] and requires them to "assess the conformity of the… high risk AI system"[1178], while protecting trade secrets.[1179]

Given that the high-risk qualification of AI scoring applications goes back to risks for fundamental rights[1180], things are even more complicated. National bodies "which supervise or enforce the respect of obligations under Union

---

[1168] Article 29(4).
[1169] Recital 80.
[1170] Article 62(3).
[1171] Regulation (EU) 2019/1020 of the European Parliament and of the Council of 20 June 2019 on market surveillance and compliance of products and amending Directive 2004/42/EC and Regulations (EC) No 765/2008 and (EU) No 305/2011 (OJ L 169, 25.6.2019, p. 1).
[1172] Recital 80.
[1173] Article 63(4).
[1174] EU Commission (2021a), Explanatory Memorandum, p. 4, recital 80.
[1175] On the new EBA guidelines on creditworthiness assessments see Feldhusen (2021).
[1176] Articles 97 to 101 of CRD IV.
[1177] Article 64(1).
[1178] Article 64(2).
[1179] Article 70(1).
[1180] See Section 5 below.

law protecting fundamental rights in relation to the use of high-risk systems" are also granted access to documents.[1181] This is restricted to "the limits of their jurisdiction"[1182] and they are to inform the market surveillance authority (hence, the financial supervisory authority) of requests they make. If they wish to test models for their impact on fundamental rights, public authorities charged with enforcing fundamental rights may make a "reasoned request" to the market surveillance authority "to organise testing of the high-risk AI system through technical means".[1183]

The penalties are considerable. Violating rules on data and data governance risks administrative fines of up to EUR 30 million or up to 6% of total worldwide annual turnover.[1184] Other rule violations face fines of up to EUR 20 million or up to 4% of total worldwide annual turnover.[1185] The supply of incorrect, incomplete, or misleading information leads to fines of up to EUR 10 million or up to 2% of total worldwide annual turnover.[1186]

It remains to be seen how happy banking regulators (and internal risk managers) will be with their new role. While regulators have so far largely left the interplay between algorithmic models, credit evaluations and scoring to the internal risk assessment of banks, this would need to change under the proposal. Supervisors will have to build proprietary expertise in the area to closely monitor AI systems. Additionally, they will have to work out a strategy for supervisory action to the extent that they are entrusted with a consumer protection mandate.[1187]

4.3 Non-banks and the risk of inconsistent regulation

Article 74 of CRD IV applies to "institutions" under the CRR. The term covers credit institutions and investment firms.[1188] Among these, the proposal's provision for special treatment as to oversight and internal risk management is restricted to credit institutions[1189] under the CRR.

It follows that non-bank entities that evaluate creditworthiness or establish credit scores do not qualify for the proposal's carve-out. This applies to companies offering essential private services such as housing, electricity

---

1181 Article 64(3).
1182 ibid.
1183 Article 64(5).
1184 Article 71(3)(b).
1185 Article 71(4).
1186 Article 71(5).
1187 For Germany see section 4(1a) of the *Finanzdienstleistungsaufsichtsgesetz*.
1188 Institutions are both credit institutions and investment firms, Article 4(1)(3) of the CRR. An investment firm is a legal person which provides investment services to third parties and/or performs investment activities on a professional basis, Article 4(1)(1) of Directive 2004/39/EC of the European Parliament and of the Council of 21 April 2004 on markets in financial instruments amending Council Directives 85/611/EEC and 93/6/EEC and Directive 2000/12/EC of the European Parliament and of the Council and repealing Council Directive 93/22/EEC (OJ L 145, 30.4.2004, p. 1).
1189 These are undertakings taking deposits or other repayable funds from the public and granting credit for its own account. See Article 4(1)(1) of the CRR.

and telecommunication[1190], and using AI systems to evaluate creditworthiness. It also applies to credit scoring agencies.

Evidently, the special regime can only cover credit institutions as far as substantive rules on internal risk management are concerned, given that non-banks do not have to provide risk-assessment structures along the lines of Article 74 of CRD IV. It is unclear whether the drafters of the proposal made a wise choice regarding the regulatory design of supervisors. Two concerns come to mind.

The first concern is that it seems that AI systems that evaluate creditworthiness or score persons are best assessed by regulators with a background in finance, rather than a more general, all-purpose regulator. A glance at US regulation in the context of credit reporting and scoring, which originated in the 1970s, offers an interesting benchmark for comparison.[1191] The Fair Credit Reporting Act[1192] (FCRA) targets the dissemination of a consumer's financial information to a third party. In that sense its policy goal resembles that of the GDPR, albeit that it covers financial data only. Consumers have the right to know what information is contained in their file, dispute inaccurate information and have it corrected, know whether their credit report was used against them and more. The FCRA also requires creditors to provide consumers with a risk-based pricing notice or an adverse action notice, in the hope of allowing improvement in their credit history.[1193] The FCRA follows a sectoral regulatory philosophy; hence, its rules are enforced by financial supervisors, namely the Federal Trade Commission and the Consumer Financial Protection Bureau (CFPB). The Dodd-Frank Act[1194] sharpened the focus by giving the CFPB the authority to supervise credit reporting bureaus and transferring rulemaking authority to this agency.[1195] Additionally, litigation offers an important means of private enforcement.

US regulators have started to consider how this regulatory framework works in the context of big data and AI. In 2020, the Board of Governors of the Federal Reserve System, the CFPB, the Federal Deposit Insurance Corporation, the National Credit Union Administration and the Office of the Comptroller of the Currency issued a "Request for Information on Financial Institution's Use of AI, Including Machine Learning".[1196] Informing credit decisions based on traditional or alternative data has been flagged as one area where the agencies wish to learn more. In line with their sectoral (i.e. not omnibus) approach, it is likely that they will be tailoring solutions to the area of financial services. As we have seen, the EU has in principle decided against a sectoral architecture, yet allows for sector-specific rules

---

1190 See Section 3.1 above.
1191 For more detail, see Langenbucher (2020).
1192 15 U.S.C. § 1681 et seq.
1193 Barr, Jackson and Tahyar (2021), p. 676 et seq.
1194 The Dodd-Frank Wall Street Reform and Consumer Protection Act of 2010 (Dodd-Frank Act), H. R. 4173.
1195 Barr, Jackson and Tahyar (2021), p. 676 et seq.
1196 Available at www.federalregister.gov/documents/2021/03/31/2021-06607/request-for-information-and-comment-on-financial-institutions-use-of-artificial-intelligence

on credit institutions. When refining the proposal, it might be worth considering further sector-specific rules. Credit scoring is one obvious candidate; evaluating creditworthiness more generally might be another one.

The second concern has to do with the risk of inconsistent regulatory standards. Banking regulators will develop one set of rules for evaluating creditworthiness and scoring in the context of banking supervision. The general AI supervisory authorities will develop another set of rules for that same purpose. This will impact competition between credit institutions and non-bank FinTechs offering similar services. Whether this creates helpful market effects or distorts competition is hard to gauge. Additionally, there is a risk of unfair results for consumers if the two sets of rules differ as to the level of protection offered.

Assessing credit scoring agencies in the context of banking supervision is outside the scope of this paper. On a side note, it is remarkable that the proposal takes a first step into an area which so far seems largely to be a regulatory void. There are no rules at European level that capture credit scoring agencies in the context of financial regulation.[1197] The Credit Rating Agency Regulation (CRAR)[1198] explicitly carves out "credit scores, credit scoring systems, or similar assessments".[1199] Not all EU Member States have credit scoring agencies, nor is there a standardised European credit scoring agency or a procedure for "translating" scores from one country to the next. Whether the fact that banks use credit scores delivered by third parties qualifies as "outsourcing" (which entails compliance requirements for credit scoring agencies) is a question of national banking supervisory law.[1200] The German Federal Financial Supervisory Authority (BaFin) has made clear that it understands credit scores as external input data and reviews them as a component of the internal rating-based approach. BaFin does not supervise credit agencies.[1201]

While there are excellent reasons to contemplate tighter regulation of credit scoring,[1202] the proposal's top-down approach and focus on AI does not seem to be ideally suited to this task. The glance at the US regulations above helped to show how credit scoring agencies trigger distinct issues

---

1197 They fall under the general rules of the GDPR (see Langenbucher (2020)). For Germany see additionally section 31 BDSG on data privacy.

1198 Regulation (EU) No 462/2013 of the European Parliament and of the Council of 21 May 2013 amending Regulation (EC) No 1060/2009 on credit rating agencies (OJ L 146, 31.5.2013, p. 1).

1199 Article 2(2)(b), recital 7 of the CRAR.

1200 The EBA does not regard market information services as outsourced activities, see EBA (2019), p. 26 (listing Bloomberg, Moody's and more). For the position under German law, see section 1(10) of the *Kreditwesengesetz*, which has, in response to the Wirecard scandal, introduced a new definition of outsourcing. The words of the rule could theoretically be read as covering some forms of scoring, however, there is no preparatory legislative material pointing in that direction. Section 88(2a) of the *Wertpapierhandelsgesetz* has, also in response to the Wirecard scandal, somewhat tightened BaFin's competencies.

1201 See statement of 23 April 2019, available at www.bafin.de/dok/12359218

1202 See Sachverständigenrat (2018).

such as data privacy, transparency, explainability and discrimination which are not limited to AI, but concern traditional agencies as well. While in the United States rules are concentrated in one legislative framework, the EU offers more of a mosaic of laws with a background in data privacy, anti-discrimination, banking supervision, and (now) AI. A focused, sectoral approach to (traditional and algorithmic) credit scoring would be a logical first step. Once put in place, the AI proposal could reference such a scoring regulation in the same way as for Article 74 of CRD IV.

5 Banking oversight and human rights

Under the proposal, AI is not the only area in which banking regulators need to build up knowledge. The benchmark for high-risk AI systems is their potential to negatively impact health, safety, or fundamental human rights.[1203] For AI systems which are intended to evaluate creditworthiness or to provide a credit score, human rights are the only relevant source of risk.[1204] It follows that banking regulators will have to supervise and offer guidance on the complicated interplay between AI fairness, statistical discrimination, macroprudential stability and internal risk management within credit institutions.

Globally, securities regulators and oversight bodies have taken the first steps towards assessing AI in that context. In January 2020, the EBA published a report on big data and advanced analytics, identifying the "four pillars" of data management, technological infrastructure, organisation/ governance and analytics methodology.[1205] Issues of trust and trustworthiness are highlighted as cutting across the four pillars. The EBA names a list of concerns including, for instance, explainability, interpretability, fairness and avoidance of bias, traceability, data protection, data quality and more.[1206] Automated credit scoring is listed as a use case in the report[1207], even if the risk the EBA identifies in the context of credit scoring is not related to discrimination. Instead, the EBA is concerned about bank staff, coaching applicants with a low credit score to game the system, thereby making the model less useful.[1208] So far, the EBA has understood its role as descriptive, refraining from policy recommendations or standard setting for supervisors.[1209]

In their 2021 supervisory principles on big data and AI, the BaFin notes that "it is essential to ensure that there are no biased results in algorithm-based decision-making processes".[1210] "Bias-based systematic discrimination of

[1203] See Section 2.4 above.
[1204] See Section 3.2 above.
[1205] EBA (2020), p. 5.
[1206] ibid., pp. 5-6.
[1207] ibid., p. 20.
[1208] ibid., p. 21; more generally on bias and discrimination see p. 37 et seq.
[1209] ibid., p. 9.
[1210] BaFin (2021).

certain groups of customers" is understood as a reputational risk.[1211] To the extent that the making of distinctions is prohibited by anti-discrimination laws, BaFin sees additional legal risks if "conditions are systematically set out on the basis of such characteristics" or if these distinctions "are replaced with an approximation".[1212] The need on BaFin's side for supervisory action is mentioned.[1213]

Worries as to risks to fundamental rights, both for data privacy and discrimination, had already been the topic of an earlier BaFin study.[1214] The agency wisely noted that the "technical challenge… is to transform the ethical/legal definition of discrimination into a mathematical one" and that there is "no currently accepted standard for non-discriminating data analysis".[1215] Under the proposal, banking supervisors and risk managers have no choice but to take up this challenge.

5.1 Why fundamental rights are different from health and safety

Some of the problems regulators might face when establishing guidance revolve around the proposal's risk-based approach.[1216] Its compliance requirements are there to mitigate specific categories of risk: namely health, safety and fundamental rights.

Product regulation provides model definitions of health and safety and a wide array of standardised norms have been developed in the past. This is not to deny that AI will give rise to enormously complex questions. However, there will usually be a clear theoretical concept of an "ideal AI system": one that poses no risk to health or safety. Cost considerations play a role, forcing us to accept a certain level of risk if the costs of avoiding it are excessive.[1217] But this does not change the ideal goal of not incurring any risk to health or safety.

For human rights, things are more complicated.[1218] At first glance, one might argue that, as with health and safety, the "ideal AI system" is one that poses no risk to fundamental rights. However, fundamental rights do not come in isolation. Protecting one fundamental right to its maximum potential will usually impact on competing fundamental rights: the protection of one right accordingly needs to be balanced against the potential risk to another. Depending on the context, the weight to be given to each human right will vary. When considering, for instance, gender

---

1211 ibid.
1212 ibid.
1213 ibid.
1214 BaFin (2018).
1215 ibid., p. 40.
1216 See Section 2.2 above.
1217 Veale and Zuiderveen Borgesius (2021) highlight the "value-laden nature" of seemingly technical standards because of such choices.
1218 Geminn (2021).

discrimination in the context of credit decisions, competing rights might include rights of other loan applicants, shareholder property rights, or rights linked to the macro-stability of financial systems. If the percentage of women eligible for a loan is lower than the percentage of women in the overall population, this might only seem like a human rights violation at first glance. A normative assessment of the women's right to equal protection against competing principles might suggest that the overall population is no adequate benchmark – a more appropriate benchmark might be the percentage of women in a comparable financial situation. Only after a balancing and weighing exercise has been carried out can we discuss the additional question of whether the costs of avoiding the remaining risk to a fundamental right are excessive.

The reason why it is more straightforward to define health and safety and more complicated to define human rights as a benchmark for risk quantification is the latter's normative nature. The way in which these two terms are defined is subject to ongoing debate and frequent reformulation. The impact of a violation of a fundamental right depends on the competing principles in question and on mitigating factors such as the availability of less discriminatory but equally useful means of achieving the desired goal. These features are characteristic of legal or ethical norms. They allow for the potential for the norms to evolve and adapt to changing societal needs. At the same time, they make those norms fluid and hard to pin down in a workable definition which could serve as a quantitative benchmark.

5.2 All bark, no bite, and the lack of private enforcement

The job of defining human rights and balancing them against competing rights has so far rested with legislators and courts, not with (banking) regulators. To take on the proposal's challenge, supervisory authorities, users and providers[1219] of relevant AI systems will have to define standards concerning what they consider a relevant human rights violation. Only then can they meaningfully quantify relevant risk. Importantly, these are normative[1220] and not quantitative questions[1221].

Today, we can only speculate how supervisors and regulated entities would go about this task. There is the theoretical possibility that credit officers and regulators will need human rights training in the future. The more likely outcome is a box-ticking exercise. Similar to AI systems in areas where EU conformity assessments exist[1222], standard setters, which are not democratically elected bodies, will develop guidance on what they consider necessary for risk management when faced with potential human rights violations. Such guidance will inform credit institutions' SREP procedures.

[1219] See EDPB-EDPS (2021) advocating for a third-party ex ante assessment.
[1220] Economists might call them "qualitative".
[1221] Gillis (2020).
[1222] See Section 2.3 above. For a critical evaluation in those areas, see Veale and Zuiderveen Borgesius (2021).

For non-banks, similar (or different!)[1223] guidance will be established, again probably by entities with little or no democratic accountability.

Taking these concerns together, the lack of private enforcement is an especially worrisome flaw in the proposal's regulatory design.[1224] The GDPR's deficiencies as to private enforcement are hinted at above.[1225] Litigating a human rights violation in a credit context is even more cumbersome, both for practical reasons, such as gaining access to information, and for intricate theoretical questions of anti-discrimination doctrine.[1226] The proposal would have offered an elegant opportunity to provide a framework for facilitating private claims in the context of creditworthiness, including legislative guidance on the disclosure of scoring models (when balanced against trade secrets), rights to explanation and rectification, contours of a business defence, and allocation of the burden of proof.[1227] In its current form under the GDPR, the proposal leaves borrowers with difficulties accessing data they would need to litigate a doctrinally difficult anti-discrimination claim.

6 Summary

This paper provides a brief overview of the use of machine learning and big data for the purposes of evaluating creditworthiness and credit scoring. It mentions the potential for inclusion which these techniques offer along with a risk of discrimination.

It moves on to discuss the Commission's proposal for an AI Act, introducing its general framework as well as specific compliance requirements for AI credit scoring and evaluation of creditworthiness which the proposal considers a high-risk system.

This paper makes two contributions to the debate.

First, it explores the proposed regulatory architecture and highlights a troubling risk of inconsistent standards between banks and non-banks. In passing, it encourages legislators to consider the regulation of credit scoring across the EU.

Second, it critically analyses the challenge of engaging in the human rights discourse banking supervisors may face under the proposal. It concludes with a comment on the lack of private enforcement options under the proposal in its current form.

1223 See Section 4.3 above.

1224 EDPB-EDPS (2021): "Blind Spot"; FRA (2020): "people need to know that AI is used, and how and where to complain", Veale and Zuiderveen Borgesius (2021).

1225 See Section 3.4 above.

1226 Langenbucher (2020). See Wachter (2021) for the argument that the ECJ's approach to anti-discrimination does not fit with algorithmic discrimination. On US doctrine of disparate impact see Barocas and Selbst (2016); Harvard Law Review (2021).

1227 EDPB-EDPS (2021); Hurlin, Pérignon and Saurin (2021).

Bibliography

Adolff, J. and Langenbucher, K. (2020), “Kreditscoring: von Auskunfteien zu künstlicher Intelligenz”, Festschrift Krieger, p. 1 et seq.

Aggarwal, N. (2021), “The Norms of Algorithmic Credit Scoring”, *The Cambridge Law Journal*, Vol. 80, p. 42 et seq.

Barocas, S. and Selbst, A. D. (2016), “Big Data’s Disparate Impact”, *California Law Review*, Vol. 104, p. 671 et seq.

Barr, M. S., Jackson Howell E. and Tahyar, M. E. (2021), *Financial Regulation Law and Policy*, 3rd edition.

Blattner, L. and Nelson, S. (2021), “How costly is Noise? Data and Disparities in Consumer Credit”, available at arxiv.org/abs/2105.07554

Boenisch, F. (2021), “Privatsphäre und Maschinelles Lernen, Über Gefahren und Schutzmaßnahmen”, *DuD*, p. 448 et seq.

Bruckner, M. A. (2018), “The Promise and Perils of Algorithmic Lenders’ Use of Big Data”, *Chicago-Kent Law Review*, Vol. 93, p. 3 et seq.

Bundesanstalt für Finanzdienstleistungsaufsicht (2018), *Big Data meets artificial intelligence – Challenges and implications for the supervision and regulation of financial services*, available at www.bafin.de/SharedDocs/Downloads/EN/dl_bdai_studie_en.html

Bundesanstalt für Finanzdienstleistungsaufsicht (2021), *Big data and artificial intelligence: Principles for the use of algorithms in decision-making processes*, available at www.bafin.de/dok/16185950

Bundesverfassungsgericht (2021), *ZD*, p. 266 et seq.

Burrell, J. and Fourcade M. (2021), “The Society of Algorithms”, *Annual Review of Sociology*, p. 213 et seq.

Djeundje, C. B., Crook, J., Calabrese R. and Hamid, M. (2021), “Enhancing Credit Scoring with Alternative Data”, *Expert Systems with Applications*, Vol. 163, 113766.

EDPB-EDPS (2021), *Joint Opinion on the proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act)*, 18 June 2021.

EU Agency for Fundamental Rights (FRA) (2020), Getting the future right – Artificial intelligence and fundamental rights, available at fra.europa.eu/en/publication/2020/artificial-intelligence-and-fundamental-rights

European Banking Authority (2019), *Final Report on EBA Guidelines on outsourcing arrangements*, EBA/GL/2019/02.

European Banking Authority (2020), EBA report on big data and advanced analytics, EBA/REP/2020/01.

EU Commission (2021a), 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, COM(2021) 206 final.

EU Commission (2021b), Impact Assessment Accompanying the 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, SWD(2021) 84 final.

European Court of Justice Case C-61/19 *Orange Romania* EU:C:2020:901.

Feldhusen, C. (2021), "Kreditwürdigkeitsprüfung: EBA-Leitlinien und nationales Recht", *WM*, p. 2020 et seq.

Geminn, C. (2021), "Die Regulierung künstlicher Intelligenz", *ZD*, p. 354 et seq.

Gillis, T. B. (2020), "The Input Fallacy", *Minnesota Law Review* (forthcoming) available at papers.ssrn.com/sol3/papers.cfm?abstract_id=3571266

Graham, J. (2021), "Risk of discrimination in AI systems, Evaluating the effectiveness of current legal safeguards in tackling algorithmic discrimination", in: Lui/Ryder, *FinTech, Artificial Intelligence and the Law*, p. 211 et seq.

Green, B. and Chen, Y. (2019), "Disparate Interactions: An Algorithm-in-the-Loop Analysis of Fairness in Risk Assessments", *FAT*19,* January 29-31, Atlanta.

Green, B. (2021), "The Flaws of Policies requiring human oversight of government algorithms", available at papers.ssrn.com/sol3/papers.cfm?abstract_id=3921216

Grützmacher, M. (2021), "Die zivilrechtliche Haftung für KI nach dem Entwurf der geplanten KI-VO", *CR*, p. 433 et seq.

Hacker, P. (2021), "A Legal Framework for AI Training Data – From First Principles to the Artificial Intelligence Act", *Law, Innovation and Technology* (forthcoming), available at papers.ssrn.com/sol3/papers.cfm?abstract_id=3556598

Harvard Law Review (2021), "Beyond intent: establishing discriminatory purpose in algorithmic risk assessment", *Harvard Law Review*, Vol. 134, p. 1760 et seq.

Hurlin, C., Pérignon, C. and Saurin, S. (2021), "The Fairness of Credit Scoring Models", *HEC Paris Research Paper No. FIN-2021-1411*, available at papers.ssrn.com/sol3/papers.cfm?abstract_id=3785882

Kiviat, B. (2019a), "The Moral Limits of Predictive Practices: The Case of Credit-Based Insurance Scores", *American Sociological Review*, Vol. 84, p. 1134 et seq.

Kiviat, B. (2019b), "The Art of deciding with data: evidence from how employers translate credit reports into hiring decisions", *Socio-Economic Review*, Vol. 17, p. 283 et seq.

Koulu, R. (2020), "Human Control over Automation: EU Policy and AI Ethics", European Journal of Legal Studies, Vol. 12, p. 9 et seq.

Landgericht Lüneburg (2021), *ZD*, p. 275 et seq.

Langenbucher, K. (2020), "Responsible A.I.-based Credit Scoring – A Legal Framework", *European Business Law Review*, Vol. 31, p. 527 et seq.

Langenbucher, K. and Corcoran, P. (2021), "Responsible AI Credit Scoring – A Lesson from Upstart.com", *European Company and Financial Law Review* (forthcoming).

Langhanke, C. (2018), *Daten als Leistung*.

Lauer, J. (2017), *Creditworthy, A History of Consumer Surveillance and Financial Identity in America.*

Oberlandesgericht Naumburg (2021), *ZD*, p. 432 et seq.

Paal, B. and Aliprandi, C. (2021), "Immaterieller Schadensersatz bei Datenschutzverstößen", *ZD*, p. 241 et seq.

Pistor, K. (2020), "Rule by Data: The End of Markets?", *Law and Contemporary Problems*, Vol. 83(2), p. 101 et seq.

Rambachan, A., Kleinberg, J., Mullainathan, S. and Ludwig, J. (2021), "An Economic Approach to Regulating Algorithms", *NBER Working Paper Series*, No 27111.

Sachverständigenrat für Verbraucherfragen (2018), *Verbrauchergerechtes Scoring, Gutachten*, available at www.svr-verbraucherfragen.de/dokumente/verbrauchergerechtes-scoring/

Spindler, G. (2021) "Der Vorschlag der EU-Kommission für eine Verordnung zur Regulierung der Künstlichen Intelligenz (KI-VO-E)", *CR*, p. 361 et seq.

Utz, C., Deleging, M., Fahl, S., Schaub, F. and Holz, T. (2019), “(Un) informed Consent: Studying GDPR Consent Notices in the Field”, available at arxiv.org/abs/1909.02638

Veale, M. and Zuiderveen Borgesius, F. (2021), “Demystifying the Draft EU Artificial Intelligence Act”, *Computer Law Review International*, p. 97 et seq.

Wachter, S., Mittelstadt, B. and Russell, C. (2021), “Why fairness cannot be automated: Bridging the gap between EU non-discrimination law and AI”, *Computer Law and Security Review*, Vol. 41, 105567.

Wagner, G. and Eidenmüller, H. (2019), “Down by Algorithms? Siphoning Rents, Exploiting Biases, and Shaping Preferences: Regulating the Dark Side of Personalized Transactions”, *The University of Chicago Law Review*, Vol. 86, p. 581 et seq.