The Human Side of Service Engineering, Vol. 62, 2022, 353–366
https://doi.org/10.54941/ahfe1002577

The Soul of a New Machine – Promises and Pitfalls of Artificial Intelligence in Finance

Christian M. Stiefmueller

CEPA | Centre for Economics and Public Administration Limited, 52 Grosvenor Gardens, London SW1W 0AU, United Kingdom

ABSTRACT

After decades of development and many false dawns Artificial Intelligence (AI), in its various guises, finally appears poised for mainstream commercial adoption. The financial sector, in particular, is looking with great interest at a broad range of applications. In April 2021, the European Commission published draft legislation that endeavours to create a comprehensive regulatory framework for the civilian use of AI. With its proposal for an 'Artificial Intelligence Act' (AI Act) the Commission aims at striking a balance between the twin objectives of promoting the uptake of AI in the European Union and the need to address the risks associated with some of its uses. To this end the AI Act identifies a number of applications that are either deemed 'high risk', and therefore subject to specific requirements and enhanced supervision, or prohibited outright. Only one of the 'high risk' applications listed in the initial proposal relates to the financial services sector. This contribution examines other potential intersections between the proposed AI Act and the extensive body of existing financial-sector legislation and seeks to provide an initial assessment of the proposed regulatory framework.

Keywords: Human side of service engineering, Financial services, Innovation, Artificial intelligence, Machine learning, Regulatory policy

INTRODUCTION

Significant advances in the development and adoption of Artificial Intelligence (AI) across a wide range of applications have confronted policymakers in many developed countries with the increasingly pressing need to update and amend their respective legislative and regulatory frameworks in response to the new challenges associated with this technology. In the European Union (EU), the Commission issued, in April 2021, a comprehensive package including a policy statement[1] and draft legislation[2] governing the use of AI. The AI Act:

[1]European Commission, Fostering a European Approach to Artificial Intelligence, Communication of the European Commission COM (2021) 205 (final), 21 April 2021.

[2]European Commission, Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act), COM (2021) 206 (final), 21 April 2021.

- provides a general definition of AI and sets out harmonised rules for the development, placement on the market and use of AI systems in the EU, including both stand-alone AI systems and systems embedded into other products;
- institutes a risk-based framework with four levels, ranging from 'minimal' to 'unacceptable risk' ('prohibited practices'), which imposes obligations upon providers and operators of AI systems in line with the risk posed by the application;
- defines harmful AI practices (Art. 5), which are prohibited outright, and 'high risk' applications (Annex III), which *'pose significant risks to the health and safety or fundamental rights of persons'* and are therefore subject to a set of mandatory requirements, including a conformity assessment, registration and continuous monitoring;
- establishes a dedicated governance system, which combines supervision at the level of EU member states, building on existing structures where possible, with the creation of a new body, the European Artificial Intelligence Board, at the EU level.

The financial services sector has been among the early adopters of data analytics and adaptive algorithms. It has also contributed a fair number of empirical case studies over the years that may hold useful lessons for the deployment of AI-enabled technologies. Nonetheless, it does not feature very prominently in the list of 'high risk' applications in the AI Act: only one financial-sector application – the assessment of creditworthiness of natural persons – is listed in Annex III of the proposal.

AI IN FINANCIAL SERVICES

This section provides a brief overview of existing and emerging applications of AI in financial services and identifies a number of known and potential future risk factors. The adoption of AI in financial services is driven by the promise of efficiency gains, which fall into two categories [OECD 2021]:

- in processing information, e.g. by assimilating more, and more diverse information more rapidly, e.g. for the purposes of assessing the risk of loan books and other portfolios of financial assets, identifying market trends and their underlying drivers, and optimising trading strategies, asset allocation and pricing; and
- in delivering services, e.g. by providing analytical input on customers' behaviour and requirements for the development and improvement of customised products and services, and by scanning activities to protect financial institutions against fraud, money laundering and cybersecurity threats.

AI in Retail Financial Services

In retail financial services, AI technology is being adopted gradually across a variety of areas. It seems appropriate to start with the assessment of creditworthiness of retail customers, which has been identified as a 'high-risk' activity in the AI Act. Consumer credit scoring has been automated for some

time in many jurisdictions, albeit to varying degrees. Most current models and services rely on structured, verified and/or quality-controlled data obtained from official sources or from dedicated private-sector service providers. Initiatives to enhance, and complement this information with non-traditional, unstructured data from other sources, such as financial transaction data shared under the 'open banking' framework and information posted on social media, are still at a relatively early stage, and the robustness of such models remains untested so far [OECD 2021].

AI-assisted product design and customization, customer profiling and product selection using 'big data', and AI-assisted pricing algorithms are also expected to become increasingly prevalent in other areas, such as property and casualty insurance, life assurance, personal investment and retirement savings products. Banks, brokers, investment managers and insurers are all required under EU law to conduct a thorough review of retail customers' economic circumstances and risk tolerance to correctly assess the suitability and appropriateness of the products and services they recommend, a complex process that is seen as a prime target for AI- assisted automation. This trend is gathering pace as retail customers become more and more used to, and comfortable with purchasing financial products and services online. So-called 'robo-advisory' services offering largely automated investment advice and portfolio management for retail investors have grown rapidly over the course of the last ten years. Machine learning already plays a significant role, which is likely to increase further as this segment matures [Maume 2021].

There is already a significant body of research looking to assess the potential risks that could arise from the deployment of AI in retail financial services, especially for consumers. With regard to consumer data and privacy, AI systems pose the same risks that are associated with data-driven business models more generally. These risks revolve mainly around the practice of collecting and analysing personal data, and the creation of personal profiles for commercial purposes, and include the unauthorised collection of such data as well as unfair and discriminatory practices in its use. Personal financial data has traditionally been regarded as inherently sensitive and afforded a higher degree of legal protection. This understanding has been called into question by initiatives, such as 'open banking' and 'open finance' that seek to make such data more readily available for commercial use [Stiefmueller 2020].

The adoption of AI technology further complicates this picture in two important ways: AI-assisted analytics significantly increase the power of algorithms to refine customer profiles by aggregating structured and unstructured data from a wide variety of sources; AI-assisted decision making and pricing algorithms apply business rules and perform calculations at higher speed, and to a deeper level of granularity than ever before. Machine learning inherently relies on probabilistic, inductive logic rather than causal deductive reasoning. Errors or biases, either in the model or in the data it relies on, can produce incorrect or discriminatory outcomes that infringe on the fundamental rights of consumers. AI-assisted systems may be entrusted with decisions, such as a bank's decision on a loan application, or advice on a life assurance policy or another retirement savings product, that may have a material impact on the consumer's life prospects or that could result in segments of the population

being systematically discriminated against, or being excluded from economic opportunities altogether [Sartor 2020]. Insights gained from customer data may also be used to exploit predictable behavioural biases and expose them to misleading, aggressive or exploitative commercial practices, such as high-pressure selling or 'bait and switch'.

Automated decision-making by AI-assisted systems, with only limited human supervision also poses problems for customers who have questions regarding the decision process or who are dissatisfied with the outcome. These problems may be amplified further if AI-assisted decision systems are supported by AI-assisted customer service desks, e.g. in the form of chatbots. Most current instances of machine learning, particularly deep learning, neural networks-based systems, create a 'black box' effect that imposes severe limitations on the transparency and explainability of the outcomes they generate. Due to the opacity of the way AI-assisted decisions are made, customer-facing personnel on the provider's side may have difficulty in justifying a particular outcome, while customers may find it difficult to establish a legal ground on which to base a potential claim, let alone obtain the documentary or other factual evidence to support it. The same opacity is also likely to cause difficulties for the suppliers and operators of AI technology – technology companies, professional services firms and providers of financial services – regarding the attribution, and delineation of their respective legal liability.

AI in the Capital Markets

In the capital markets, quantitative investment management, based on the statistical analysis of economic and market data, emerged in the late 1980s, drawing on advances in financial theory, the availability of large volumes of data, rapid increases in computing power and the development of new financial instruments, especially derivatives. Initially, these algorithms were static and had to be updated and recalibrated manually to incorporate significant new information or re-assessments of market conditions or economic trends. The shortcomings of automated, but static 'programme trading' became apparent as early as 1987 when 'portfolio insurance', a risk-hedging algorithm developed by Berkeley academics Hayne Leland and Mark Rubinstein, was found to have played a major role in that year's U.S. stock market crash. Ten years later, Long-Term Capital Management (LTCM), a hedge fund with Nobel laureates Myron Scholes and Robert C. Merton Miller on its board of direc-tors, that mainly pursued strategies known as 'convergence trades', collapsed in the wake of the 1998 financial crisis in Russia. The demise of LTCM was linked to limitations in the company's quantitative models, which failed to adequately account for rare, low-probability / high-impact events, such as financial crises. In May 2010, the so-called 'flash crash', which saw the market value of leading U.S. equity indices decline by nearly 10 per cent. in a matter of minutes, was attributed, primarily, to market manipulation, in particular by 'spoofing' algorithms, amplified by high-frequency trading. Since then, advances in AI technology have raised expectations that machine learning algorithms could improve the accuracy of predictive models and

enable algorithmic investment and trading strategies to better respond and adapt to market developments. This has led to the widespread adoption of AI-assisted decision-making tools among investment managers, particularly hedge funds. In addition to the generation of investment ideas and the construction of portfolios, AI is also used increasingly in risk management and in the routing and execution of trades [OECD 2021].

There are, however, concerns that the widespread adoption of AI may not materially reduce the underlying risks associated with the large-scale automation of capital markets activity but, to the opposite, could render these vulnerabilities even more acute. International institutions, such as the FSB [FSB 2017] and the OECD [OECD 2021], have highlighted a number of potential risks associated with the mainstream adoption of AI technology in the capital markets that could be grouped into three categories:

- Financial stability (systemic) risks: the adoption of AI models could lead to market participants pursuing increasingly similar trading strategies, which could, in turn, result in increased market volatility, procyclicality and herding behaviour;
- Market manipulation (integrity) risks: predictable patterns in the behaviour of automated trading strategies, and the availability of AI-assisted analytical tools, could be exploited by insiders or cybercriminals to manipulate market prices. On the other hand, AI-driven investment and trading could also result, even unintentionally and unknown to their operators, in collusion and the manipulation of market prices, if algorithms were to engage in co-operative, profit-maximising strategies that would be unlawful for a human market participant, but may not be legally attributable, or even detected, when executed by an algorithm; and
- Market structure (competition) risks: as observed in other markets before, digitalisation tends to produce concentrated outcomes due to a combination of technical standardisation, network effects, and economies of scale. Initially, at least, the level of financial resources and human capital required to adopt AI technology or use big data information sources in-house is likely to favour larger market participants and provide them with an advantage over smaller competitors. Over time, there is a risk that a majority of capital market participants could come to rely on a small number of providers of AI technology and services, or become dependent on data sources controlled by a few major digital platform operators.

Money Laundering and Financial Crime

Static, rules based alert systems have also been in use for some time now to detect and prevent money laundering, terrorist financing, and other criminal activities, such as fraud. These systems fulfil two main purposes: on the one hand customer risk rating models support the customer due diligence ('Know Your Customer', KYC) process and create customer risk profiles whenever a new client relationship is formed; on the other hand, fraud detection software scans transactions, such as payments, transfers or securities order flow, on a continuous basis to detect and re-port suspicious patterns. Institutions are also working on the integration of the latter, in particular, with their general

cybersecurity defences in order to better detect and address various kinds of malicious activity on their networks. Technology providers and institutions have high hopes for machine learning to improve the accuracy of these systems [IBM 2019]. One of the most frequently cited shortcomings of existing anti-money laundering (AML) systems, and systems for combating the financing of terrorism (CFT) and other financial crime, is their tendency to produce 'false positives', which can be very disruptive for both customers and institutions. As mentioned previously, AI algorithms are at risk of developing discriminatory biases, which could be difficult to detect and/or remedy. A 'false positive' during the KYC process could result in a potential customer being denied the right to open a bank account. If several institutions were to source their systems from the same supplier and/or calibrate them using similar training sets, they would likely produce similar, negative outcomes, leaving potential customers, in particular vulnerable groups, such as migrants and other persons living in precarious economic conditions, permanently excluded from basic financial services.

SCOPE OF EU REGULATORY FRAMEWORKS

Fundamental Rights

As mentioned previously, the fundamental rights of EU citizens are enshrined in, and protected by, the EU Charter of Fundamental Rights. The rights to privacy (Art. 7) and data protection (Art. 8) are implemented, and made enforceable in EU secondary law by the General Data Protection Regulation (GDPR[3]). With respect to the use of AI, Arts. 21 and 22 GDPR place limits on profiling and automated decision-making: Art. 21 grants citizens a right to object against profiling based on personal data. while Art. 22 states that citizens have the right *'not to be subject to automated decision making, including profiling,'* which produces legal effects or otherwise significantly affects them and/or their personal interests. In both cases, exemptions apply where the use of this data *'is necessary for entering into, or the performance of, a contract'* between the citizen and, e.g. a provider of financial services (Art. 6(1) lit. b and Art. 22(2) lit. a GDPR). The boundaries of what is deemed 'necessary' – in view of the general principles set out in Art. 5(1) GDPR, particularly the principles of 'fairness and transparency' (lit. a) 'purpose limitation' (lit. b) and 'data minimisation' (lit. c) – will likely be drawn over time by the European Data Protection Board (EDPB), and the EU and national courts. Two additional pieces of legislation that aim at establishing general rules for data-sharing between government and the private sector, the Data Governance Act[4] and the European Data Act[5], are currently being discussed by the EU legislators.

[3]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 (General Data Protection Regulation, GDPR), OJ L 119, 04 May 2016.

[4]European Commission, Proposal for a Regulation of the European Parliament and of the Council on European data governance (Data Governance Act, DGA), COM (2020) 767 (final), 25 November 2020.

[5]European Commission, Proposal for a Regulation of the European Parliament and of the Council on harmonised rules on fair access to and use of data (Data Act), COM (2022) 68 (final), 23 February 2022.

Whereas the EU Charter of Fundamental Rights contains a general ban on discrimination on the grounds of sex, race, colour, ethnic or social origin, genetic features, language, religion or belief, political or any other opinion, membership of a national minority, property, birth, disability, age or sexual orientation (Art. 21), this provision has long been considered as practically unenforceable by individual citizens, especially in the context of disputes between private parties arising from contractual relationships. Only recently, the EU courts have accepted a direct application by EU citizens[6], albeit in a different context [Leczykiewicz 2020]. Whether discriminatory commercial practices, e.g. in connection with the use of AI, may at some point be adjudicated directly by the courts under the scope of Art. 21 remains uncertain at this stage [Helberger et al. 2020]. Legal remedies that are available in EU secondary law (see below), are more specific and limited in scope.

Finally, the adoption of AI technology, and especially the 'black box' effect associated with current machine-learning models, also raises issues regarding the right to effective legal redress, which is also protected by the EU Charter of Fundamental Rights (Art. 47). As mentioned previously, the lack of transparency of the process by which decisions are made is likely to make it difficult for users to identify a potential infraction of their rights, in the first place, to engage with the provider, e.g. by way of a formal complaint, and, finally, to pursue legal remedies through the courts. This is an intrinsic flaw of most current AI systems that might, and should be addressed by further technical development that concentrates on improving the transparency and explainability of machine-learning algorithms. In the meantime, reversing the 'burden of proof' against AI-assisted decisions in favour of the individual claimant could gone some way towards mitigating the 'black box' effect and incentivising suppliers and operators to apply adequate conformity testing and risk management procedures.

Consumer Protection Laws

In EU law, consumers are defined as natural persons acting in a non-professional capacity (Art. 3 Consumer Credit Directive, CCD[7]). EU secondary legislation in general, and consumer protection law in particular, contains an array of measures, such as a ban on unfair commercial practices, information and disclosure obligations, and duties of care. Cornerstones of EU consumer protection law that are applicable to financial services are the Unfair Commercial Practices Directive (UCPD[8]), the Unfair Terms Directive (UCTD[9]), and the Distance Marketing of Financial Services Directive

[6] Court of Justice of the European Union (CJEU), Cases C-569/16 and C-570/16 *Stadt Wuppertal v. Maria Elisabeth Bauer* and *Volker Wilmeroth v. Martina Broßonn*, ECLI:EU:C:2018:871.

[7] Directive 2008/48/EC of the European Parliament and of the Council of 23 April 2008 on credit agreements for consumers, OJ L 133, 22 May 2008, pp. 66–92.

[8] Directive 2005/29/EC of the European Parliament and of the Council of 11 May 2005 concerning unfair business-to-consumer commercial practices in the internal market, OJ L 149, 11 June 2005, pp. 22–39.

[9] Council Directive 93/13/EEC of 05 April 1993 on unfair terms in consumer contracts, OJ L 95, 21 April 1993, pp. 29–34.

(DMFSD[10]). The UCPD, in particular, bans (a) misleading practices that rely on information that is false or deceptive and '*causes or is likely to cause [the consumer] to enter into a transaction that he would not have taken otherwise*' (Art. 6); and (b) aggressive practices that '*significantly impair the average consumer's freedom of choice or conduct*' (Art. 8).

The proposed AI Act would complement the existing EU consumer protection law in two important ways. On the one hand, the AI Act, as a regulation, would be directly applicable in all member states and grant citizens rights that are directly enforceable in court, both at the national and the EU level (Art. 263(4) TFEU) – unlike most of the existing body of EU consumer protection law, which is framed as directives and implemented by the member states through national legislation; on the other hand, it comprises a list of 'prohibited practices' (Art. 5), which expands on the UCPD to ban specific practices, including the use of subliminal techniques (para. 1) and the exploitation of vulnerabilities due to age, physical or mental disability (para. 2) '*in order to materially distort a person's behaviour in a manner that causes or is likely to cause that person or another person physical or psychological harm*'. The limitation to 'physical or psychological harm' is problematic, however, and should be amended to include the equally important dimension of economic harm.

Another relevant aspect in this context is the possibility of using AI technology for personalised pricing, which is the subject of intense discussion [Helberger et al. 2021, Sartor 2021]. There is broad agreement, however, in favour of a duty to disclose the use of personalised pricing to consumers. According to Art. 7(4) lit. c UCPD and Art. 3(1) lit. 2b DMFSD the price to be paid by the consumer for a product or service forms part of the material information which should generally be provided to the customer in advance of any contractual agreement. Both provision state that, if the price cannot be calculated reliably in advance, at least the manner in which it is calculated should be disclosed. Neither seems to imply a duty to disclose to the consumer the use of a personalised pricing algorithm [Jablonowska et al. 2018]. Art. 52 AI Act contains a generic obligation that '*AI systems intended to interact with natural persons are designed and developed in such a way that natural persons are informed that they are interacting with an AI system, unless this is obvious from the circumstances and the context of use.*' This obligation falls short of addressing the main issue, which is to inform customers not only of the fact that they are facing an AI-assisted system but, most importantly, what purpose that system serves. This information should be part of all relevant disclosure obligations.

Financial Sector Regulation

In addition to general consumer protection law, the deployment of AI-assisted systems in financial services should, *a priori,* comply with the relevant sectoral frameworks. EU financial services regulation applies the principle of

[10]Directive 2002/65/EC of the European Parliament and of the Council of 23 September 2002 concerning the distance marketing of consumer financial services (Distance Marketing of Financial Services Directive, DMFSD), OJ L 271, 09 October 2002, pp. 16–24.

technology neutrality, which is often summarised with the phrase '*same activity, same risk, same rules*'. This means that the same set of statutory rules applies to financial services and transactions, no matter what type of technology is used. If new technologies are used to deliver or support certain financial services that are subject to, e.g., MiFID II[11], the established rules apply, nevertheless [Maume, 2021]. With the introduction of potentially disruptive technologies, such as AI, this principle should prompt a thorough review of the adequacy of the existing frameworks.

The only sectoral framework that is mentioned expressly in the proposed AI Act is the Capital Requirements Directive (CRD V[12]), which, together with the Capital Requirements Directive (CRR II[13]), regulates credit institutions (banks) and large investment firms. For AI-assisted systems that are provided or used by regulated credit institutions, the competent authorities who are responsible for their regular, prudential supervision would also be tasked with supervising the application of the AI Act (Art. 9(9) AI Act) on the grounds that the management of AI systems should form part of the institution's internal governance and risk management processes. While banks usually conduct credit scoring for their own internal purposes, usually for mortgage or small business loans, other entities, such as credit bureaus, provide credit scores as a commercial service. Such scores are frequently used to assess creditworthiness in the context of consumer loans (Art. 8 CCD[14]). Under the Commission's proposal, these entities would be supervised by the national authority that has been charged with the implementation of the AI Act across all sectors other than banking. There is a risk that the respective technical and implementing rules and guidelines that will be developed over time by financial supervisors on one side, and AI/data protection authorities on the other, could diverge, which could lead to a significant degree of legal uncertainty for businesses and consumers alike [Langenbucher 2020].

Another important application that is currently not classified as 'high risk' in the AI Act – but should arguably be – is the assessment of suitability and appropriateness, which plays a central role in the area of retail investments, personal savings and pensions, and insurance. Each of these sectors is governed by a legal framework that sets out requirements, processes, and procedural safeguards. The most relevant of them, in this context, are the Markets in Financial Instruments Directive (MiFID II), which applies for most investment products, and the Insurance Distribution Directive (IDD[15]), which governs the selling of insurance products. The rules for suitability

[11]Directive 2014/65/EU of the European Parliament and of the Council of 15 May 2014 on markets in financial instruments (MiFID II), OJ L 173, 12 June 2014, pp. 349–496.

[12]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(CRD V), OJ L 176, 27 June 2013, pp. 338–436.

[13]Regulation (EU) 575/2013 of the European Parliament and of the Council of 26 June 2013 on prudential requirements for credit institutions and investment firms (CRR II), OJ L 176, 27 June 2013, pp. 1–337.

[14]Directive 2008/48/EC of the European Parliament and of the Council of 23 April 2008 on credit agreements for consumers (CCD), OJ L 133, 22 May 2008, pp. 66–92.

[15]Directive (EU) 2016/97 of the European Parliament and of the Council of 20 January 2016 on insurance distribution (IDD), OJ L 26, 02 February 2016, pp. 19–59.

assessments under Art. 25 MiFID II and Art. 30 IDD, including a number of delegated acts and regulatory guidelines, have been amended and updated in recent times to account for the adoption of digital technologies. Legislators and supervisors seem to be well aware of the risk posed to customers, particularly retail customers, by the increasing use of automation. It would only be consequent, therefore, to classify AI-assisted systems used in the context of suitability and appropriateness assessments as 'high risk' in the AI Act, and their supervision should be assigned to the competent financial authorities, e.g. under Art. 36 Investment Firms Directive (IFD[16]).

The process of customer due diligence for the purposes of assessing the risks of money-laundering and terrorist financing (AML/CFT) is governed in the EU by Arts. 13–18a AMLD 5[17]. This area has been an early focal point for the deployment of data analytics and other digital technologies to deal with the diversity and complexity of the data that may be required to complete the assessment to a reliable standard, and the significant reputational and economic risk to the financial institution from failing to do so. As mentioned previously, the outcome of this process is often decisive for the ability of individuals to access to basic financial services, such as a current bank account, which, if wrongfully denied, could have a severe negative impact on the economic and life prospects of that person. It is important, therefore, to ensure that AI-assisted systems used for this purpose are free from fault or unlawful biases. They should be classified as 'high risk' for the purposes of the AI Act and included in Annex III.

Market Integrity and Competition

Largely autonomous, AI-assisted trading algorithms may involve significant risks to market integrity. In the EU, algorithmic trading is governed, in particular, by Art 17 MiFID II and the relevant technical standards of the European Securities and Markets Authority (ESMA), while general safeguards against market manipulation and other threats to the integrity of the capital markets are provided by the Market Abuse Regulation (MAR[18]). Art. 12 MAR lists a number of manipulative practices while Art. 15 MAR contains a general ban on any (natural or legal) person to '*engage in or attempt to engage in market manipulation*'. Predictably, the current legal position raises difficult questions of attribution and liability. As in all of the previous examples, the activity of the AI systems must be attributable to a natural or legal person to establish liability. Due to the 'autonomy' of the system – always granted to it, and delineated by human decision-makers, of course – and the 'black box' character of most machine-leaning algorithms

[16]Directive (EU) 2019/2034 of the European Parliament and of the Council of 27 November 2019 on the prudential supervision of investment firms, OJ L 314, 05 December 2019, pp. 64–114.

[17]Directive (EU) 2018/843 of the European Parliament and of the Council of 30 May 2018 amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing (Anti-Money Laundering Directive, AMLD 5), OJ L 156, 19 June 2018, pp. 43–74.

[18]Regulation (EU) No 596/2014 of the European Parliament and of the Council of 16 April 2014 on market abuse (Market Abuse Regulation, MAR), OJ L 173, 12 June 2014, pp. 1–61.

this attribution is becoming increasingly tenuous [Azzutti et al. 2021]. At present, supervisors rely, to a large extent, on internal risk management processes and self-assessment prepared by the supervised firms themselves. Regulators have recognised the need for supervisors to become more involved, e.g. by conducting a formal review of firms' self-assessments [ESMA 2020].

As the use of AI-assisted systems becomes more prevalent Art 17(2) MiFID II may need to be revised to require regular external assessments, e.g. by the supervisor. Suppliers and operators are obliged, already now, to disclose algorithms for supervisory and enforcement purposes by virtue of Arts. 17(2) and 69(2) MiFID II. These obligations should be operationalised by including regular reviews into the review and evaluation process. The adoption of AI technology by financial market participants will place an increasing burden on the competent supervisory authorities more generally, not only in terms of capacity but also with respect to the skill sets required from their staff and the technical tools at their disposal. So-called 'guardian' AI systems that test and analyse other AI systems to identify non-compliant behaviour [Sartor 2020], as well as AI systems that trace and visualise the logical processes of machine-learning algorithms to render them more transparent and explainable, should be considered and evaluated as part of a nascent arsenal of Supervisory Technology (SupTech) to assist authorities with these tasks.

The integrity of the financial markets could be negatively affected by the effects of concentration, e.g. among providers of AI technology or suppliers of 'big data'. In the EU, the proposed Digital Markets Act[19], which aims at placing restrictions on the ability of large digital platform providers ('gatekeepers') to leverage their market position across sectors, would go some way towards mitigating the impact of network effects and preventing excessive concentration of data, and therefore market power, in the hands of a small number of market participants. Potential systemic risk arising from a concentration of processing and analytical services would be addressed, at least partially, by the forthcoming Digital Operational Resilience Act (DORA)[20], which includes a framework for the direct supervision of 'critical third-party providers of ICT services' by financial-sector authorities.

DORA also requires financial institutions to strengthen their defences against financial crime and cybersecurity risks, which could also become a source of contagion and destabilise the financial system. To reflect the rising importance of AI in this respect, Art. 4(2) DORA should be amended to ensure that the responsibility of the management body of a financial entity includes the operational and legal integrity of any AI-assisted system it operates.

[19]European Commission, Proposal for a Regulation of the European Parliament and of the Council on contestable and fair markets in the digital sector (Digital Markets Act, DMA), COM (2020) 842 (final), 15 December 2020.

[20]European Commission, Proposal for a Regulation of the European Parliament and of the Council on digital operational resilience for the financial sector (Digital Operational Resilience Act, DORA), COM (2020) 595 (final), 24 September 2020.

CONCLUSION

The proposed AI Act would mark an important step towards improving legal certainty and setting out a comprehensive framework for the deployment of this technology in the EU. Regarding the financial sector, in particular, a number of issues need to be recognised:

- The definition of 'prohibited practices' (Art. 5 AI Act) does not account for economic harm, which can be as much of a threat to the life prospects of citizens as physical and psychological harm, and which is the main risk that users of financial services are exposed to.
- The list of high-risk applications (Annex III) should be expanded accordingly, and include the use of AI-assisted systems in suitability and appropriate assessments for retail customers (MiFID II and IDD), and customer risk assessments for AML/CFT purposes (AMLD 5).
- The 'black box' character of present-day machine-learning algorithms places retail customers, in particular, at a massive disadvantage when required to formulate, and prove, a claim against an AI-assisted decision. As long as AI-assisted decision-making processes remain opaque and lack explainability, reversing the 'burden of proof' in favour of the individual should be an option.
- Given the built-in characteristic of machine-learning systems to adapt their behavior over time, operators should be obliged to carry out regular benchmarking exercises against dedicated, standardised reference datasets to identify modelling biases and other issues. These exercises should be reviewed by independent experts and/or the competent supervisor.
- The supervision of AI systems in financial services should be integrated with sectoral supervision. Integrated supervision of AI, as well as other ICT risks, should not be limited to banking but is equally important in the securities, asset management and insurance sectors.
- Reviews of AI-assisted systems should become part and parcel of the supervisory review and evaluation process across all financial sectors. The use of AI-enabled supervisory technologies (SupTech) should be considered and evaluated in this context.

The examples discussed in this article only provide a snapshot of legal issues emerging from the adoption of AI in the financial sector in Europe. Further research and discussion between legislators, supervisors, industry participants and civil society will be required to achieve an outcome that takes into account the rapid technological progress, and a balance of interests that reflects the EU's stated commitment to the human-centric, values-based use of technology.

REFERENCES

Aggarwal, N. 2019, 'Machine Learning, Big Data and the Regulation of Consumer Credit Markets: The Case of Algorithmic Credit Scoring', in N. Aggarwal, H. Eidenmüller, L. Enriques., J. Payne & K. van Zwieten (eds), *Autonomous Systems and the Law*, C.H. Beck/Nomos, Munich/Heidelberg, pp. 37–44.

Azzutti, A., Ringe, W.-G. & Stiehl, H.S. 2021, *Machine Learning, Market Manipulation and Collusion on Capital Markets: Why the 'Black Box' Matters*, EBI Working Paper Series No. 84, European Banking Institute, Frankfurt.

Bertrand, A., Maxwell, W. & Vamparys, X. 2021, 'Are AI-based Anti-Money Laundering (AML) Systems Compatible with European Fundamental Rights?', *International Data Privacy Law*, vol. 11/3, pp. 276–293.

Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) 2021, *Big Data and Artificial Intelligence: Principles for the Use of Algorithms in Decision-Making Processes*, Bundesanstalt für Finanzdienstleistungsaufsicht, Bonn/Frankfurt.

Cambridge Centre for Alternative Finance (CCAF) & World Economic Forum (WEF) (2020), *Transforming Paradigms: A Global AI in Financial Services Survey*, University of Cambridge/World Economic Forum, Cambridge/Geneva.

European Securities and Markets Authority (ESMA) 2020, *Consultation Paper: MiFID II/MiFIR Review Report on Algorithmic Trading,* ESMA70-156-2368, 18 December 2020, European Securities and Markets Authority, Paris.

Expert Group on Liability and New Technologies - New Technologies Formation 2019, *Liability for Artificial Intelligence and Other Emerging Digital Technologies*, European Union, Luxembourg.

Financial Stability Board (FSB) 2017, *Artificial Intelligence and Machine Learning in Financial Services. Market Developments and Financial Stability Implications,* FSB, Basel.

Floridi, L., Holweg, M., Taddeo, M., Silva, J. A., Mökander, J. & Wen, Y. 2022, *capAI - A Procedure for Conducting Conformity Assessment of AI Systems in Line with the EU Artificial Intelligence Act*, Said Business School, Oxford.

Hacker, P. 2018, 'Teaching Fairness to Artificial Intelligence: Existing and Novel Strategies against Algorithmic Discrimination under EU Law', *Common Market Law Review*, vol. 55, pp. 1143–1185.

Helberger, N., Lynskey, O., Micklitz, H.-W., Rott, P., Sax, M. & Strycharz, J. 2021, *EU Consumer Protection 2.0. Structural Asymmetries in Digital Consumer Markets. Joint Report from Research Conducted under the EUCP 2.0 Project*, European Consumer Organisation (BEUC), Brussels.

Independent High-Level Expert Group on Artificial Intelligence (HLEG AI) 2019, *Policy and Investment Recommendations for Trustworthy AI,* European Commission, Brussels.

International Business Machines (IBM) 2019, *Fighting Financial Crime with AI. How Cognitive Solutions are Changing the Way Institutions Manage AML Compliance, Fraud and Conduct Surveillance*, White Paper, IBM Corporation, Armonk, NY.

Jabłonowska, A., Kuziemski, M., Nowak, A. M., Micklitz, H.-W., Pałka, P. & Sartor, G. 2018, *Consumer Law and Artificial Intelligence. Challenges to the EU Consumer Law and Policy Stemming from the Business Use of Artificial Intelligence. Final Report of the ARTSY Project*, EUI Working Paper Law 2018/11, European University Institute, Florence.

Langenbucher, K. 2020, 'Responsible A.I.-based Credit Scoring – A Legal Framework'. *European Business Law Review*, vol. 31/4, pp. 527–572.

Leczykiewicz, D. 2020, 'The Judgment in Bauer and the Effect of the EU Charter of Fundamental Rights in Horizontal Situations', *European Review of Contract Law,* vol. 16/2, pp. 323–333.

Maume, P. 2021, *Robo-advisors. How do they fit in the existing EU regulatory framework, in particular with regard to investor protection? Study for the Committee on Economic and Monetary Affairs*, European Parliament, Luxembourg.

Organisation for Economic Cooperation and Development (OECD) 2021, *Artificial Intelligence, Machine Learning and Big Data in Finance. Opportunities, Challenges and Implications for Policy Makers*, OECD, Paris.

Organisation for Economic Cooperation and Development (OECD) 2020, *Financial Consumer Protection. Policy Approaches in the Digital Age*. OECD, Paris.

Prenio, J. & Yong, J. 2021, *Humans Keeping AI in Check – Emerging Regulatory Expectations in the Financial Sector*, FSI Insights on Policy Implementation No. 35, Bank for International Settlements, Basel.

Sartor, G. 2020, *New Aspects and Challenges in Consumer Protection. Digital Services and Artificial Intelligence. Study for the Committee on the Internal Market and Consumer Protection*, European Parliament, Luxembourg.

Stiefmueller, C.M. 2020, 'Open Banking and PSD 2: The Promise of Transforming Banking by Empowering Customers', in J. Spohrer & C. Leitner (eds.), *Advances in the Human Side of Service Engineering. Proceedings of the AHFE 2020 Virtual Conference on The Human Side of Service Engineering, July 16-20, 2020*, Springer, Cham, pp. 299–305.