Routledge
Taylor & Francis Group

Law and Financial Markets Review

ISSN: (Print) (Online) Journal homepage: https://www.tandfonline.com/loi/rlfm20

Banking on AI: mandating a proactive approach to AI regulation in the financial sector

Jon Truby , Rafael Brown & Andrew Dahdal

To cite this article: Jon Truby , Rafael Brown & Andrew Dahdal (2020) Banking on AI: mandating a proactive approach to AI regulation in the financial sector, Law and Financial Markets Review, 14:2, 110-120, DOI: 10.1080/17521440.2020.1760454

To link to this article: https://doi.org/10.1080/17521440.2020.1760454

Published online: 15 May 2020.

Routledge
Taylor & Francis Group
Law and Financial Markets Review, 2020
Vol. 14, No. 2, 110–120, https://doi.org/10.1080/17521440.2020.1760454

Banking on AI: mandating a proactive approach to AI regulation in the financial sector*

JON TRUBY

Centre for Law & Development, College of Law, Qatar University, PO BOX 2713, Doha, Qatar

RAFAEL BROWN

Centre for Law & Development, College of Law, Qatar University, PO BOX 2713, Doha, Qatar

ANDREW DAHDAL

Centre for Law & Development, College of Law, Qatar University, PO BOX 2713, Doha, Qatar

Despite an emerging international consensus on principles of AI governance, lawmakers have so far failed to translate those principles into regulations in the financial sector. Perhaps, in order to remain competitive in the global race for AI supremacy without being typecast as stifling innovation, typically cautious financial regulators are unusually allowing the introduction of experimental AI technology into the financial sector, with few controls on the unprecedented risks to consumers and financial stability. Once an unregulated AI software causes serious economic harm, a public and regulatory backlash would lead to over-regulation that could harm innovation of this potentially beneficial technology. Artificial intelligence is rapidly influencing the financial sector with innumerable potential benefits, such as enhancing financial services and improving regulatory compliance. This article argues that the best way to encourage a sustainable future in AI innovation in the financial sector is to support a proactive regulatory approach prior to any financial harm occurring. This proactive approach should implement rational regulations that embody jurisdiction-specific rules in line with carefully construed international principles.

Declarations

List of abbreviations

Anti-Money Laundering (AML)
Artificial Intelligence High-Level Expert Group (AI HLEG)
Artificial Intelligence (AI)
Fair Credit Reporting Act (FCRA)
Financial technologies (FinTech)
General Data Protection Regulation (GDPR)
RegTech (Regulatory Technology)

I. Introduction

As traditional forms of financial activity change, technology is heralding an important transition for financial institutions from human-centred to computer-centred financial services.[1] The gradual transition towards a computer and data-driven financial industry can already be seen in the rapid growth of the financial technologies (FinTech) sector. This transition also means that financial institutions must adapt their business models, computer systems, and distribution networks[2] to emerging realities. Even the most fundamental prevailing paradigms informing financial regulation now require rethinking.[3]

One of the emerging grand challenges in this transitional period is the integration of artificial intelligence (AI) into the existing systems and processes of financial institutions. Among the plethora of issues that need to be tackled are third party vendor management, data ownership, privacy, ownership rights, costs, and cybersecurity.[4] Faced with the opportunities and challenges posed by AI, banks and other financial players face a slow, lengthy, risky, and potentially very costly transition and integration process.[5]

Governments will need to craft and adopt policies and regulations to facilitate this significant transition. Building the regulatory infrastructure requires that policymakers work with technology experts to understand, manage and control the risks posed by AI in the digital, physical, economic, and political spheres.[6] Being at the cusp of this revolution, now is the time for financial institutions to consider both

**AI governance in the financial sector based on internationally accepted principles.*

the positive and negative aspects of AI. On the one hand, financial institutions must assess how AI may increase efficiencies in the financial industry including enhanced fraud detection, more accurate lending and credit assessments, stronger cybersecurity detection, faster regulatory compliance and overall better trading and investment decisions. On the other hand, financial institutions also need to consider how AI will create inherent risks and threats.

Within this risk-benefit matrix, this study examines three distinct contexts wherein AI can and is being utilised in the financial sector.

1. It looks at how financial service providers use AI in relation to their clients.
2. It looks at how financial services firms use AI in their compliance efforts.
3. Finally, it examines how regulators use – and may use – AI in their regulatory efforts.

In recent years, various international principles on AI governance have crystallised. Individual jurisdictions, however, have been slow or cautious to translate any such principles into hard law. This reluctance may be due to either regulatory inertia or a fear of losing the global race for AI supremacy by appearing hostile to AI.[7] Financial regulators are by nature cautious and generally prioritise risk control over support for financial innovation. They are mandated with systemic stability and consumer protection and this posture characterises their approach to new developments. A prime example currently playing out in many jurisdictions is the cautious approach financial regulators have taken towards digital currencies and Initial Coin Offerings.[8]

Despite the risks, developers and financial institutions in many jurisdictions are generally free to experiment with AI-led technology in the financial sector within the scope of their existing licenses. AI developers and the financial institutions are therefore experimenting with AI technology largely outside specific regulatory parameters. Financial intuitions are introducing a plethora of AI-driven financial services, including robo-advising, algorithmic investing and insurance/credit assessment at a rapid pace and as a first generation technology. Though governed by existing financial and data protection laws, neither the developers nor the financial institutions have significant legal obligations in any jurisdiction to follow the international principles on AI governance.[9] These principles have been developed to require accountability, transparency, explainability, and fairness in the utilisation of AI software in the financial sphere.

This article argues that it is prudent and timely for regulators to seriously consider the nature and scope of AI regulation in the financial services sector. The adoption of rational regulations that encourage innovation whilst ensuring adherence to international principles will significantly reduce the likelihood that AI-related risks will develop into systemic problems. Leaving the financial sector only with voluntary codes of practice may encourage experimentation that in turn may result in innovative benefits – but it will definitely render customers vulnerable, institutions exposed and the entire financial system weakened. Should an AI-induced systemic shock similar to the GFC strike the global economic system, the resulting knee-jerk regulatory backlash against AI would set and stifle AI innovation curtailing the real benefits and potential of AI in the financial sector. As such, this article argues that it would be optimal for policymakers to intervene early with targeted, proactive but balanced regulatory approaches to AI technology in the financial sector that are consistent with emerging internationally accepted principles on AI governance. The article goes on to explain that balancing the risks of AI with the benefits of innovation requires addressing macro and micro level details.

II. Defining AI

Defining AI is no easy task[10] because there is no agreed upon definition. However, articulating a working, albeit non-exhaustive, definition of AI is necessary for a productive analysis. The coining of the term "artificial intelligence" is credited to John McCarthy in a proposal for a Dartmouth summer conference in 1956.[11] Since then, over 70 definitions have been proposed.[12] While the word "artificial," which, in this context, essentially refers to "machines" or "computers", is quite easy to define, it is in defining the word "intelligence" that experts cannot agree. One definition suggests that intelligence in AI means an artificial entity that can "function appropriately and with foresight" in a given environment.[13] Others define or measure intelligence with reference to human intelligence or performance, while others define intelligence with reference to the artificial entity's ability in terms of thought process or behaviour.[14] A simplistic way of conceptualising AI is to think of it simply as a software or a set of computer programmes that allow for considerable improvements in computer or machine programmes and processes over time.[15] Thus far, no AI has reached human level intelligence, referred to as artificial general intelligence. However, a number of AI programmes have exceeded human performances in specific tasks, including computational and predictive financial modelling.[16]

Machine learning, which is a large field of study but is only one of a number of sub-fields within AI, are AI programmes that can self-learn from a given set of data.[17] Most of what people refer to as AI today is actually machine learning, which consists of feeding data into an algorithm that can then make inferences, predictions, and models common in the big data driven financial sector.[18] Within the field of machine learning, and an important distinction in the finance sector, are programmes that are "supervised" or "unsupervised." Supervised learning involves a set of correct answers that accompany data input, while unsupervised learning involves systems that self-identify data patterns that could be unstructured.[19]

For purposes of this article, we define AI as a suite of autonomous self-learning and adaptively predictive technologies that enhances the ability to perform tasks.[20]

III. AI in financial services

As part of the broader FinTech (re)evolution, the use of AI has developed in the financial sector in five main areas[21]:

1. compliance;
2. fraud and anti-money laundering (AML) detection;

3. lending and credit assessments;
4. cybersecurity; and
5. trading and investment decisions.

Innovations are often born after a crisis, as deficiencies become evident in the resulting wash-up. The main cause of large-scale financial crises are typically the same as those that traditionally and historically affect commercial banks: poor internal governance.[22] Many factors characterise poor internal governance. Poor credit control, connected lending, and insufficient liquidity and capital can all lead to increased risk-taking and market instability.[23] In turn, the primary aim of financial regulation is to maintain market stability, protect investors, and prevent abuses and the escalation of uncontrolled risks.[24] In this regard, financial regulation is complex, imperfect, and often reactive.[25] The 2007–2008 global financial crisis laid bare the shortcomings of regulators for mishandling the crisis, including their tolerance for risks created by global current-account imbalances that further inflated the US housing bubble.[26] In its aftermath, regulators reacted with a substantial, and often unpredictable,[27] increase in financial regulation.[28] Post-crisis financial regulations have upended the financial sector, changing its system of operation, risk-taking, and profitability.[29] Most notably, post-crisis financial regulations have become increasingly burdensome in terms of compliance, cost, and penalties.[30]

A. The "FinTech and RegTech" paradigm

FinTech emerged with the aim of enhancing the delivery of financial products, services, and solutions. Examples of FinTech include crowdfunding, digital (crypto) currencies, and peer-to-peer lending.[31] The ubiquity of FinTech has both revolutionised finance and created new regulatory challenges. The role of financial regulation is therefore far from over, especially in this new era as the financial sector transitions its products, services, processes, and systems to embrace new technologies. Regulators are now scrutinising the myriad of points where financial services intersect with technological innovation. Among those coming under the microscope are the three (interconnected) "big whales" of FinTech: big data, AI, and cybersecurity.[32]

Technology is also revolutionising regulatory compliance. In recent years, technological solutions have emerged to address the ever increasing demands of and need for regulatory compliance. This area, which according to Arner et al is distinct from FinTech, has been termed "RegTech" (referring to the convergence of regulation and technology). RegTech is the use of technology, including AI, for all manner of legal compliance, including financial regulatory compliance, reporting, and monitoring.[33] We agree with Arner et al that RegTech will change the very foundations of financial services regulation because of the need for a more dynamic rather than a reactive regulatory system.[34] RegTech will allow financial institutions to better control risks and lower regulatory compliance costs. At the same time, RegTech will allow regulators to monitor dynamically and predict more accurately the effects of regulatory reforms on financial markets.[35]

It is within this brave new "FinTech and RegTech" paradigm that AI discourse within the financial services sector exists. The three dimensions where AI is having, and is expected to have, the greatest impact are in the delivery of financial services, the regulation of financial entities and compliance with legal obligations in the financial services sector.

B. AI and the delivery of financial services

Of all financial services contexts, advisory services and the ability to deliver valuable, tailored and informed financial advice to customers has the greatest potential to benefit from AI technology.[36] Conversely, it is also the context where some of the greatest risks to customers associated with the use of AI can be realised.

1. Lending decisions

Financial institutions increasingly use AI to determine lending risks, and to help assess the credit worthiness of applicants across a range of services. For example, AI has been used to predict the likelihood of credit card default payments by customers.[37] Additionally, banks use AI to collect information about customers, including financial transactions,[38] spending habits, geolocations, account details, and social media data. The collection and input of customer data into an AI system creates a curated or targeted ecosystem[39] that financial institutions could use algorithmically to increase customer loyalty. AI can also make predictions about customer behaviour and help banks arrive at decisions about credit worthiness or even the interest rate offered to a specific loan applicant. More controversially, AI also has the potential to predict the creditworthiness of applicants despite lack of any credit history by using a so-called "alternative data". Alternative data refers to information that is publically available such as public records, social media posts[40] and even online transaction history shared by online venders who have been given permission by applicants[41] (usually via a dense EULA[42]).

Hypothetically, AI driven credit score systems could be fully automated producing in-depth personalised analysis and instantaneous decisions based on collated online data and traditional credit-scoring techniques.[43] As discussed further below, Article 22 of the EU's GDPR framework mandates that no such human-absent system is permitted to make such decisions.

2. Trading and investment advice

Financial institutions are also using AI to help make trading and investment predictions and decisions. AI software is being used in research, for example, by mining data to gain sectoral insights that can derive actionable data points. Through the examination of masses of information and the derivation of seemingly unrelated correlations (for example correlating weather patterns with the demand for a commodity such as ride-sharing services (eg. Uber)) or even the independent improvement of search and prediction algorithms, AI has the potential to create significant value in the trade and investment space. Advice can also be tailored to match customer risk profiles and thresholds again informed by algorithmic assessments of customer data.

The idea of AI-powered "self-driving finance" that automates the role of the financial advisor (creating so-called

"robo-advisors") is already a service that many financial firms have rolled out. Customers in many jurisdictions are therefore already engaging with "AI-agents" that can help compare, personalise, and recommend financial products and services.[44]

3. Customer service

Financial services are becoming increasingly consumer-centric with the help of AI. Financial institutions are using AI to create customer experiences that are less sterile (a sentiment often associated with banking), more engaging and personal. For example, many financial (and indeed non-financial) institutions are using AI "chat-bots" to assist online customers with queries and respond to simple requests. Lloyds Banking Group, for example, has invested billions into a curated ecosystem that uses data from consumers, corporate clients, and third parties to create a comprehensive financial experience that targets specific consumer needs as or when (or even before) they arise.[45]

As with all uses of AI, the core consideration is personal data privacy, protection, and its management. Enhanced customer services and products require the financial sector to further rely and entrust AI systems and algorithms with sensitive personal data.

C. Regulation and compliance

Financial institutions are already using AI to automate compliance efforts.[46] This is in addition to other innovative "RegTech" compliance-assistive technologies being used, including smart contracts and blockchain.[47]

As discussed previously, the substantial increase in complex and constantly changing myriad of post-crisis regulations, such as the BASEL III liquidity and capital regulations, Dodd-Frank, and GDPR, requires compliance officers to review and keep up with regulations and documents pertaining to multiple jurisdictions.[48] Compliance and reporting by financial institutions, and supervision by regulators, have all become ever more frequent, precise, and detailed.[49] Compliance costs for regulated entities are growing (as are fines for non-compliance), but the costs involved in supervision by regulators are also significant.[50]

AI software allows financial institutions to better and more efficiently assess, monitor, and report compliance risks. Internal enterprise information can also be monitored and analysed in real time.[51] Experts predict that the automated RegTech compliance paradigm will one day be the norm for both regulators and financial institutions, leading to a continuous and real-time reporting and monitoring process with global scope.[52]

Banks are also enhancing their fraud and AML detection systems with AI algorithms. Anomaly detection using AI based software makes fraud detection faster and cheaper.[53] The use of AI in AML and fraud detection has been very helpful for financial institutions, which are required by law to report instances of fraud or money laundering. The use of non-AI, rules-based systems to detect fake accounts and flag suspicious transactions, on the other hand, is much slower and generates a number of false positive results.[54] Furthermore, autonomous AI agents, that are both reactive and proactive, are being deployed to get ahead of the ever-changing methods used by money launderers. When combined with the use of a multiple AI agent architecture, it has been proven that AML detection becomes more effective.[55] While the autonomous AI agent approach is gaining momentum, in a technical sense, AML detection still ultimately requires human AML expert review and final decision-making.[56] Once the technology develops, however, policy makers will face the dilemma of whether the removal of humans from the detection process is desirable.

IV. The emerging international consensus?

The current state of global AI regulation remains at the policy level. Several jurisdictions have published positions papers and policy documents on AI, addressing how to balance the benefits and risks.[57] The introduction of rules and laws governing AI raise difficult practical and philosophical questions.[58] In recent years, several legal systems around the world have begun to grapple with these tensions. One of the first movers and clear leaders in the AI race (if not the race for AI regulation) is China. In 2017, the Chinese government outlined its plans to be the global power in AI technology by 2030.[59] Other jurisdictions, such as India, have sought to develop AI to assist in human development – a so-called "AI for All" approach.[60] In February 2019, US President Donald Trump issued an Executive Order designed to maintain US technological superiority in the AI sphere.[61] As one expert asserts, however, "[no] country has a coherent strategic approach to governance and regulation of AI yet."[62]

In deference to the potentially revolutionary impact of AI, the OECD has established an international working group that has recently released proposed principles on AI governance that could subsequently apply to AI regulation.[63] Members of the G20 have adopted the principles outlined in that document.[64] Furthermore, in April 2019, the Artificial Intelligence High-Level Expert Group (AI HLEG) under the auspices of the European Commission released its own AI regulation strategy document titled "Ethics Guidelines for Trustworthy AI."[65] These guidelines are designed to inform legal reforms in the EU concerning the use of AI. They emphasise many of the elements discussed above with respect to transparency, privacy and the importance of user consent when deploying AI. This ultimately involves implementing procedures to ensure AI operates within boundaries of accountability, transparency, explainability, and fairness to guarantee trustworthiness.[66]

Between the OECD and the EC's AI HLEG, a core set of principles seem to be emerging with respect to the regulation of AI. These core elements include the following:

1. Human agency and oversight
2. Robustness and safety
3. Privacy and data governance
4. Diversity, non-discrimination and fairness
5. Transparency
6. Societal and environmental well-being
7. Accountability

These principles reflect a certain level of universality. In whole or in part, several aspects and elements of these

principles are echoed in various AI global policy statements such as the Japanese Society for Artificial Intelligence Ethical Guidelines.[67] A proposal for federal algorithmic auditing, which the US Senate Intelligence Committee adopted to guarantee unbiased algorithmic decision-making, also includes similar philosophical goals.[68]

The clearest and strongest manifestation of AI regulation is Article 22 of the EU's General Data Protection Regulation (GDPR).[69] Applying not only to EU member states, but also to all entities dealing with the data of EU citizens, GDPR is a far-reaching transnational regulatory framework. Titled "Automated individual decision-making, including profiling", Article 22 provides as follows:

1. The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her.
2. Paragraph 1 shall not apply if the decision:
   (a) is necessary for entering into, or performance of, a contract between the data subject and a data controller;
   (b) is authorised by Union or Member State law to which the controller is subject and which also lays down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests; or
   (c) is based on the data subject's explicit consent.

Given the relative novelty of Article 22, concepts such as "legitimate interest" and "necessity for entering a contract" have yet to be fully developed.

V. Risks of unregulated AI in the financial sector

A. The AI regulatory challenge

The impetus to issue stringent regulations governing AI development and deployment in the financial sector will arise because of an economic systemic shock attributed to lax AI oversight, or because of risk averse policymakers taking a proactive regulatory posture. At the moment, it appears as if the latter is the most likely scenario. One of the problems with a proactive approach, however, is calibrating the appropriate level of regulatory magnification. Should regulators focus their efforts on macro-level risks as guided by aggregate concerns, or should they take a more granular micro-level approach by focusing on the conduct of individual AI operators? Further yet, are both levels of operation inextricably linked?

One of the lessons from the 2008 financial crisis was that hubris can be catastrophic. Many financial market players believed they had overcome risk itself through a sophisticated system of lightning trades and derivatives markets.[70] The near divine capabilities being attributed to AI raise the real prospect that, a decade on from the Great Recession, complacency may be returning and financial regulators need to ready.

AI is quite possibly the most innovative technology presently being developed – or indeed, that has ever been developed.[71] Regulation runs the risk, therefore, of stifling this monumental innovative push. The problem of regulation, as noted above, has significant geo-political ramifications.[72] AI is the newest frontier of an active front in the great race for global economic supremacy. Regulation of AI, as far as it could slow down the pace of development, will face strong opposition given the stakes at play. Balancing the risks of AI with the benefits of innovation requires addressing macro and micro level details. Concurrently, policy makers must acknowledge the potential global significance of the sector in formulating their regulatory frameworks.[73]

1. AI regulation at the macro level

At the macro level, AI has the capability to enhance significantly the regulatory toolbox available to policymakers.[74] The ability to identify anomalies, patterns or trends through the analysis and cross-referencing of large data sets[75] provides a powerful mechanism for regulators seeking systemic stability. Indeed, the risk of systemic instability is actually growing as economies are increasingly data-driven and that data is increasingly interconnected. The prospect of contagion is now a real risk with far-reaching disruptive potential given the extent to which data is wedded together across systems and sectors.[76] As financial systems develop and continue to become intertwined across jurisdictions, instability or uncertainty infecting one area can quickly spread across the network. These ripples may be technical glitches arising from technological failures, but they are just as likely to be financial problems caused by improper practices or processes.

Whereas in the past, Keynes lamented that economic sentiments were driven by "animal spirits", today – and moving forward into the future, that sentiment may well evolve so that rather than "animal spirits", it will be "artificial systems" that drive economic sentiment. As the technology develops, and the ability of laymen to understand the underlying processes become more and more tenuous, the distinction between the mysterious "animal spirits" and ubiquitous "artificial systems" may well collapse. Transparency is, therefore, another fundamental pillar of AI regulation.

The dream of any regulator (honest with themselves) is undoubtedly absolute control. AI represents a step forward towards that dream.[77] The ability to monitor – in real time – the transactions and financial flows coursing through an economy, will allow regulators to rapidly identify and act to avert broad financial risks. Being able to initially articulate those risks so as to set parameters for the AI system (such as consumer credit vs aggregate household income) will still be an important human element for any automated monitoring system. With machine learning, however, the system in time may augment existing parameters or even set new parameters signifying systemic risk. In this extended realm of machine-generated activity, concepts of fault and liability become much more difficult to navigate.[78]

AI can also increase productivity and efficiency in the regulatory process by automating key data-driven regulatory processes. The monitoring of money laundering and potential terrorist financing activities is a prime area where AI can make a significant difference in the near term.[79] For regulators, the problem of "false-positives" in AML/CTF projects, for example, is a drain on resources and a material inconvenience

to regulated entities. Reducing the number of times that legitimate transactions are incorrectly flagged as suspicious will enhance confidence in regulation, and minimise wasted time and resources.

2. AI regulation at the micro level

In these early stages of AI development, discourse surrounding the regulation of AI in the financial sector, has been focused on the control of enterprise level deployment of the technology. There is, of course, a significant and growing body of work on the use of AI (and other technologies) *in* regulation (RegTech).[80] The clear confluence of attention however, has been directed towards the regulation *of* AI as and when deployed by market participants.

The discussion in the financial context regarding which particular activities or processes ought to be regulated focusing mainly on the use of client data. These regulatory "pain points" can be summarised into three categories:

(i) Bias and discrimination in financial decision making
(ii) Model risk management based on data sets and consequent liability
(iii) Cybersecurity, data privacy and transparency in data sources

Each one of these categories is examined below.

a. Anti-discrimination in the delivery of financial services AI is a double-edged sword in many respects. By leveraging masses of data and being able to cross-compile traceable details, AI can enhance choices and outcomes through tailored and personalised services. The dark side of all these potential benefits are unintended discrimination or bias in the delivery or financial services, and a decline in user privacy.[81]

Most developed and developing jurisdictions around the world have some kind of anti-discrimination framework.[82] Such regimes render it unlawful to deny government (or even private sector) services to a person based on some arbitrary characteristic such as their race, sex, or religion. The risk for AI is that datasets upon which AI systems base their decisions may unintentionally contain these biases skewing future decision one way or another.[83] Indeed, the Hong Kong Monetary Authority has proposed tools in its White Paper for banks to detect and correct biases in algorithmically-determined decisions.[84]

In lending and credit decisions, this risk has been a principal concern of stakeholders concerned with the rise of AI in the financial sector.[85] For example, an AI system could correlate the default rate arising from a dataset with the addresses of defaulting parties. This data point could adversely impact otherwise viable applicants based on their place of residence. The connection between socio-economic status and locality need not be explained. The outcomes, therefore, may hinder the potential for economic mobility arising from the extension of bank credit without considering the individual circumstance of the applicant. An AI system that is independent from human intervention and that interacts with clients directly (via online portals or Apps) may filter out potential applicants based on ostensibly correct information from a statistical perspective – but results in an outcome that is otherwise unjust or unfair. AI "profiling" can embed existing human prejudices into its automated algorithmic decision-making and in AI-led recommendations to human decision-makers following statistical analysis.[86] This can happen either through analysis of accurate statistical factors which lead to detrimental outcomes for profiled candidates, or because the data itself has been collated incorrectly through human prejudices (such as higher arrests of ethnic communities based on police discrimination).[87]

In the insurance sector, particularly life insurance, similar decisions may arise through the crystallisation of data-points based on correlations most people would consider unpalatable.[88] For example, certain racial groups may be prone to given health conditions above and beyond the general population. Insurance companies could use that information to deny coverage to that individual based on the increased propensity of people of that ethnic extraction to suffer from that given condition.

The role of AI regulation in the financial context would be to attempt to extend fair-lending criteria and anti-discrimination laws to the realm of AI derived decisions. It is highly improbable that any firm would deliberately programme an AI system to exhibit explicit and outward bias. The risk, therefore, is that the internal development or machine learning of the system itself may bring to the fore truths and realities that society considers objectionable.[89] Regulators would then have to impose politically motivated value judgements on the outer parameters of AI activities. The penumbra created at this juncture represents one of the most conceptually challenging aspects of regulating AI. What some may see as an objective and value-neutral system, may inevitably become politicised.

b. AI model risk management regulation Model risk refers to the dangers associated with the creation of market models that produce actionable outputs. Particularly relevant to financial advisors, AI powered models would produce data that will be used to advise or service clients in relation to allocation of investment funds. AI systems could model various trends and risk variables in order to produce investment strategies that match the risk profile of a particular client.

The regulatory challenge in this context is overcoming the "black box" phenomenon. That is, the basis upon which that advice was given needs to be verifiable to determine whether an advisor has satisfied their fiduciary duty to the client. Does the advice, for example, avoid conflicts of interest between the advisor/advisory firm and the target of the investment upon which the advice was given? Can the advice be reconciled as being fair and reasonable and appropriately suited to the client to which it was directed?

The problem can be summed up with the term "explainability".[90] The core question is whether the information produced through the AI system can be explainable within the realm of regulation.

This also raises the question of liability with respect to who is at fault when inadequate advice was rendered.[91] Can the programmer of an AI investment platform be liable for data produced by a system whose parameters they did not set?[92] The initial parameters informing the model design may be visible, but what happens when the system itself "improves" those parameters autonomously? Imposing liability on the

system owner or first mover will again hamper innovation, as AI systems will be purposefully handicapped to remain always under the supervision and control of the human agent. The potential gains from AI are once again stumped.

There have been cases where financial advisors have been held accountable for the investment models produced by their computers. In one case such liability was said to arise because the controlling advisor wrongly deleted a risk control parameter and this was concealed from advisory clients.[93] In another ongoing case, London's commercial court will hear a case beginning April 2020 where a client lost $20 million due to the trading decisions of a financial institution's algorithm.[94]

The interesting element in examining the parameters set for an AI system is that those parameters reveal the intentions of the organisation or entity employing AI technology (in a criminal context: *mens rea*). In a sense, this may make the task of regulators easier in that the (original) AI parameters will reflect whether a firm is blindly profit-maximising or whether the parameters embody the considerations legally incumbent on financial advisors. No regulated firm will likely be naive enough to programme a robotic advisor to blindly pursue profit maximisation at all costs – yet this may only mean that more nuanced subterfuge need now be detected by regulators.

The design and parameters loaded into an AI model are therefore a window into the proverbial soul of the operations of a financial enterprise. Although regulations may require that the soul be pure, it will only be through an examination of AI system parameters that an ultimate judgement may be cast.

c. Cyber security, data privacy and transparency One of the strongest justifications offered by firms for the collection of data from consumers is that such data allows service providers to tailor their service and improve user experience and outcomes. In the world of finance, data is increasingly being used to realise disintermediation. In many financial relationships, consumers can now independently drive and complete their own financial decisions. From credit, to investments to insurance, data driven systems are empowering customers.

The autonomy derived, however, does not diminish the level of responsibility expected from financial service providers. The nature of those responsibilities have now shifted to emphasise the key elements of privacy and transparency in relation to the data that is now at the core of the sector.[95]

The accumulation of data, and the ability to connect, cross-reference and monetise that data creates dangerous risks. The "honey pot" idea refers to the risk posed by nefarious operators seeking to unlawfully access personal data. If all information is accumulated in a single system, criminals only need target one single point of vulnerability for a potentially massive pay off. Should they succeed in accessing this one single system, essentially all the information relating to all clients can be accessed. There is little doubt of the benefits of having all data concentrated within a single system, but the consequences of a data breach of that single system can be catastrophic.

Data should also not be kept private from those to whom it refers. In the US, for example, the Fair Credit Reporting Act (FCRA)[96] is designed to ensure that the data collected by credit rating agencies is accurate and up to date. Transparency is vital in order that errors within a data set relied upon by an AI systems can be corrected. Clients should be made aware of not only data breaches, but also what exact data is being used to generate important and personalised decision documents such as credit reports. If the system is using so-called "alternative data" – data scraped from social media or other non-official sources – clients should be allowed to know where that data came from, and address its implications or inconsistences.[97] Laws like the FCRA will become increasingly important with the proliferation of AI and data driven finance.

Transparency in data also allows those to whom data driven decisions will be made to confirm the "data-hygiene" of the accumulated information. This would mean examining all aspects of the accuracy of accumulated information ensuring its currency, relevance and completeness. Information that is incomplete, out of date, or ostensibly irrelevant should not be inputted into an AI system in order to derive vital consumer information or make consumer related decisions.

The maintenance of data, therefore, is important from a consumer protection perspective as well as a cybersecurity perspective. Regulatory structures relating to AI driven decision-making ought to focus on data that is to be ultimately fed into the AI system. AI regulations concerning financial firms, therefore, should require high levels of data control and curation in order to ensure complete and up-to-date information and to avoid potentially unjust errors. At the same time, the masses of data collected need to be stored and maintained within a system design that is strong enough to withstand prevailing cyber threats.

The key to consumer fairness is transparency. In recognition of this fundamental aspect of AI, in Europe, GDPR restricts the process of automated decision making based on the processing of personal data if that process is to result in any legal effects.[98] If such a process is to take place, GDPR provisions require that it be explicitly consensual, necessary to perform the contract to which it refers, and is authorised by national law.[99]

The privacy aspect of AI is not limited to the privacy of clients or users. Given the nature and potential intrusiveness of AI-powered regulation, employee privacy may become an increasingly important issue.[100] The privacy of employees is an evolving aspect of labour law around the world. Although privacy issues can generally be addressed through the employment contract, the nature of regulatory oversight that AI systems can produce raises the stakes. AI-powered systems can scan and monitor written and even verbal communication between a financial service provider and client in order to determine whether the voice or language used embodies any duress, predatory practise or other undue and unlawful pressure. The data collected and retained would constitute a significant sample of the speech of any single target of such regulation.[101] The voice and communication data produced would also conceivably require storage by regulators such that it might be used in any future litigation or enforcement action – or even to address subsequent complaints by clients. How regulators themselves are to deal with this information is itself an important regulatory question.

VI. The importance of consistent AI regulation (or the risk of an unbalanced approach)

The discussions above illustrate the vast potential benefits and serious risks associated with the use of AI in the financial sector. As AI technology develops, policymakers will be tasked with balancing innovation with potential risks to the public good. Any attempt at manipulating the future regulation of AI to preference one stakeholder at the expense of others will likely result in damaging market distortions in the financial sector. The emerging AI regulatory consensus as embodied in the documents recently produced by the AI HLEG and the OECD provides a clear regulatory path that, if implemented, should be implemented uniformly. AI regulation in the financial sector must balance all three contexts in which AI is used to avoid "distorted" and "unbalanced" outcomes (defined below). AI regulation ought to be applied consistently and equally to (1) financial firms using AI to provide financial services, (2) firms using AI for regulatory compliance, and (3) regulators using AI for monitoring.

If one is to speak of "market distortions", "skewed outcomes" and "regulatory imbalance" it is vital to clearly articulate the meanings of these expressions. The following discussion, therefore, spells out the potential risks to the core AI regulatory principles connected with an AI regulatory posture that is variously favourable to either regulators, firms (in compliance) and firms (in service deliver) and explains the consequences of such a narrow approach.

(i) AI regulations favourable/permissive to regulators over other stakeholders

Should lawmakers regulate AI in a way that favours regulators and their ability to wield AI technology to its full power (i.e. exempting AML detection AI systems from human oversight), the broad risk posed is one of economic waste. The losses to the economy stem from an automated AI system that is devoid of the nuances required of modern regulation. An unleashed regulatory AI system that is unsupervised by human regulators and does not respect data privacy principles (in that it can scrape, cross-reference and analyse swathes of online user data from all available sources) has the potential to hurt more than it would help the economy and economic agents. Financial market participants operating under such conditions may well face random automated intrusive regulatory interference and be required to answer for circumstances and situations that a human agent may have understood to be acceptable.[102]

(ii) AI regulation favourable/permissive to firms in the context of regulatory compliance

Enhancing compliance with the law is hard to argue against. Yet when that compliance is done in a way that lacks transparency, reduces human accountability and engenders complacency, legal compliance loses its meaning. Where a compliance framework powered by an AI system sends data to a regulator, and that data is not curated or even handled by a human agent associated with the regulated firm, that firm will inevitably have its culture of compliance eroded. Compliance requires accountability, transparency and answerability. Where an autonomous AI system in effect shields the firm from day to day compliance those virtues will become martyrs to progress.

(iii) AI regulation favourable/permissive to firms in the context of service delivery

Data protection laws are perhaps the most important in the context of AI systems used to provide clients with financial services. The main risks are that firms who possess and manage this data for the purpose of feeding it into the AI system will be lax with that information. An unregulated AI in financial service delivery also allows for potential discriminatory outcomes. The solution to this challenge seems to be the need for human oversight concerning certain decisions. Lack of regulation in the use of AI in service delivery also poses more heightened cybersecurity risks, especially when financial firms lack guidance as to the incorporation of AI into their cybersecurity policies and physical networks. Such enterprise-level risks also hold the potential to become catastrophic systemic risks affecting entire financial markets.

VII. Conclusion

AI has great potential in enhancing financial services and regulatory compliance. As technical developments progress and policymakers begin to think about hard law regulations, the key question is one of balance. The core principles of AI regulation embodied in OECD and EC documents represent as good a starting point as any. How that starting point will be translated into jurisdiction specific laws will require consideration of the risks of AI against the potential for innovation that AI holds. As financial market policymakers grapple with these elements, the interests of stakeholders must also be considered. For the benefit of such policy makers, this article has sought to identify those stakeholders, explore the nature of their interests and outline their exposure to the risks and benefits involved with the growth of AI technology.

An unregulated approach might very well create a Wild West environment that exposes the systemically vital financial sector to risk and uncertainty. Over-regulation, by contrast, may stifle innovation and comparatively disadvantage the aspirations of a jurisdiction at the cusp of the "fourth industrial revolution".

The nature, level and applicability of AI regulation in the finance sector will need to balance and combine a constellation of interests and considerations. The identified core principles of AI regulation that are emerging on the international stage provide a useful compass. In addition to these core principles (transparency, accountability, data protection and privacy), it is important that lawmakers craft consistent and equally applicable regulatory frameworks that place all stakeholders in the financial sector on a level AI playing field. ■

ORCID

Jon Truby http://orcid.org/0000-0002-9184-7033
Rafael Brown http://orcid.org/0000-0001-6751-7176
Andrew Dahdal http://orcid.org/0000-0002-1436-1486

Funding

This publication was made possible by the NPRP award NPRP 11S-1119-170016 from the Qatar National Research Fund (a member of The Qatar Foundation). The statements made herein are solely the responsibility of the author.

Jon Truby, PhD, Associate Professor of Law and Director of the Centre for Law & Development, College of Law, Qatar University. jon.truby@qu.edu.qa; https://www.linkedin.com/in/jon-truby-b7042166/

Rafael Brown, JD, Clinical Assistant Professor of Law, Centre for Law & Development, College of Law, Qatar University.

Andrew Dahdal, PhD, Assistant Professor of Law, Centre for Law & Development, College of Law, Qatar University

Notes

1 RM Lacasse, BA Lambert, E Osmani, C Couture, N Roy, J Sylvain, and F Nadeau, "A Digital Tsunami: FinTech and Crowdfunding", International Scientific Conference on Digital Intelligence, Quebec City, Canada, April 4–6, 2016, available at http://fintechlab.ca/wp-content/uploads/2016/11/Digital-Tsunami-Site-Web.pdf [accessed 21 Aug 2019].

2 Lacasse, *supra* n 1.

3 DW Arner, J Barberis, and RP Buckley, "FinTech, RegTech, and the Reconceptualization of Financial Regulation", (2017) 37 *Nw. J. Int'l L. & Bus.* 371 (arguing that RegTech will mean a paradigm shift in financial regulation).

4 R Bharadwaj, "AI for Cybersecurity in Finance – Current Applications", Emerj (19 June 2019), available at https://emerj.com/ai-sector-overviews/ai-cybersecurity-finance-current-applications/ [accessed 21 Aug 2019].

5 *Ibid*.

6 JC Newman, "Toward AI Security: Global Aspirations for a More Resilient Future", CLTC White Paper Series (Feb 2019), available in pdf at https://cltc.berkeley.edu/wp-content/uploads/2019/02/CLTC_Cussins_Toward_AI_Security.pdf [accessed 21 Aug 2019].

7 F Westerheide, *The Artificial Intelligence Industry and Global Challenges*, Forbes, Nov 27, 2019, https://www.forbes.com/sites/cognitiveworld/2019/11/27/the-artificial-intelligence-industry-and-global-challenges/#5597aeb53deb.

8 J Truby, "Fintech and the City: Sandbox 2.0 Policy and Regulatory Reform Proposals", (2018) *International Review of Law, Computers & Technology*, https://doi.org/10.1080/13600869.2018.1546542.

9 J Jagtiani and K John, "Fintech: The Impact on Consumers and Regulatory Responses", (2018, November–December) 100 *Journal of Economics and Business* 1–6, https://doi.org/10.1016/j.jeconbus.2018.11.002; LD Wall, "Some Financial Regulatory Implications of Artificial Intelligence", (2018 November–December) 100 *Journal of Economics and Business* 55–63, https://doi.org/10.1016/j.jeconbus.2018.05.003.

10 *Ibid* (calling it "notoriously difficult to define").

11 G Press, *Artificial Intelligence (AI) Defined*, Forbes Magazine (Aug. 27, 2017), available at https://www.forbes.com/sites/gilpress/2017/08/27/artificial-intelligence-ai-defined/#1f22b88f7661 (accessed 6 Sept. 2019); Newman, *op. cit.* n 6.

12 S Legg and M Hutter, "A Collection of Definitions of Intelligence," arXiv, June 15, 2007, https://arxiv.org/pdf/0706.3639.pdf.

13 NJ Nilsson, *The Quest for Artificial Intelligence: A History of Ideas and Achievements* (Cambridge University Press 2010).

14 SJ Russell and P Norvig, *Artificial Intelligence A Modern Approach* (Prentice-Hall, Inc. 1995), http://www.cin.ufpe.br/~tfl2/artificial-intelligence-modern-approach.9780131038059.25368.pdf.

15 Newman, *op. cit.* n 6.

16 K Grace, et al., "When Will AI Exceed Human Performance? Evidence from AI Experts," arXiv, May 3, 2018, https://arxiv.org/pdf/1705.08807.pdf (last accessed 4 November, 2019).

17 Newman, *op. cit.* n 6.

18 *Ibid*.

19 *Ibid*.

20 Deloitte, *The New Physics of Financial Services: How Artificial Intelligence Is Transforming the Financial Ecosystem*, available in pdf at https://www2.deloitte.com/qa/en/pages/financial-services/articles/artificial-intelligence-transforming-financial-ecosystem-deloitte-fsi.html (accessed 9 Sept 2019). See also, A Baker, RS Eisner, JM Pennell, and EA Raymond, *Investing In AI Fintech Companies* in *Artificial Intelligence & Financial Services*, Mayer Brown (Spring 2019), available in pdf at https://www.mayerbrown.com/-/media/files/perspectives-events/events/2019/04/article-booklet.pdf (accessed 9 Sept 2019).

21 Bharadwaj, *op. cit.* n 4.

22 C Goodhart, P Hartmann, D Llewellyn, L Rojas-Suarez, and S Weisbrod, *Financial Regulation: Why, how and where now?* 2 (Routledge: 1998).

23 *Ibid*.

24 CK Whitehead, *Reframing Financial Regulation*, 90 (Boston Univ. L. Rev. 6 2010) (arguing that financial markets have begun to bypass traditional business categories that largely frame financial regulation due to convergence in the products and services, new market entrants, and a shift in capital-raising and risk-bearing from traditional intermediation to the capital markets); J Black, *Restructuring Global and EU Financial Regulation: Character, Capacities, and Learning* 1.06 in E Wymeersch, KJ Hopt, and G Ferrarini (eds.), *Financial Regulation and Supervision: A Post-Crisis Analysis* (Oxford University Press 2012).

25 Whitehead, *op. cit.* n 21; Black, *op. cit.* n 21.

26 The Economist, *The Origins of the Financial Crisis*, Sep 7th 2013, https://www.economist.com/schools-brief/2013/09/07/crash-course.

27 Black, *op. cit.* n 21.

28 DW Arner, J Barberis, and RP Buckley, "FinTech, RegTech, and the Reconceptualization of Financial Regulation", (2017) 37 *Nw. J. Int'l L. & Bus.* 371.

29 *Ibid*.

30 Arner et al., *op. cit.* n 25; P Treleaven and B Batrinca, "Algorithmic Regulation: Automating Financial Compliance Monitoring and Regulation Using AI and Blockchain", (2017) 45 *J. of Fin. Transformation* 14, 15.

31 Arner et al., *op. cit.* n 25.

32 E Ossawa, *Three Whales of FinTech: AI, Big Data and Cybersecurity*, 8allocate, available at https://8allocate.com/article/three-whales-of-fintech-ai-big-data-and-cybersecurity/ (accessed 10 Sept. 2019).

33 Arner et al., *op. cit.* n 25. Also described as "technological solutions to regulatory processes." INST. OF INT'L FIN., REGTECH: EXPLORING SOLUTIONS FOR REGULATORY CHALLENGES 2 (Oct. 2015).

34 Arner et al., *op. cit.* n 25.

[35] *Ibid*.
[36] See also, DA Zetzsche, DW Arner, RP Buckley, and B Tang, *Artificial Intelligence in Finance: Putting the Human in the Loop* (February 2020). CFTE Academic Paper Series: Centre for Finance, Technology and Entrepreneurship, no. 1. Available at SSRN: https://ssrn.com/abstract= at p.17.
[37] Bharadwaj, *op. cit.* n 4.
[38] Deloitte, *The New Physics of Financial Services: How Artificial Intelligence Is Transforming The Financial Ecosystem*, available in pdf at https://www2.deloitte.com/qa/en/pages/financial-services/articles/artificial-intelligence-transforming-financial-ecosystem-deloitte-fsi.html (accessed 9 Sept 2019) (Companies like Comply Advantage, for example, use AI-based algorithms to monitor transactions).
[39] *Ibid*.
[40] Bharadwaj, *op. cit.* n 4.
[41] I Kerr and J Earle, (2013–2014) 66 *Stan. L. Rev.* Online 65, "Prediction, Preemption, Presumption: How Big Data Threatens Big Picture Privacy", at 69.
[42] End User License Agreement.
[43] MS Caron, "The Transformative Effect of AI on the Banking Industry", (2019) *Banking & Finance Law Review* 34(2), 169–214. Retrieved from http://0-search.proquest.com.mylibrary.qu.edu.qa/docview/2207836906?accountid=13370, at p.180; see also Financial Stability Board, *Artificial Intelligence and Machine Learning in Financial Services: Market Developments and Financial Stability Implications* (2017) at p.18.
[44] Deloitte, *op. cit.* n 34.
[45] *Ibid*.
[46] Bharadwaj, *op. cit.* n 4.
[47] P Treleaven and B Batrinca, "Algorithmic Regulation: Automating Financial Compliance Monitoring and Regulation Using AI and Blockchain", (2017) 45 *J. of Fin. Transformation* 14, 15.
[48] Bharadwaj, *op. cit.* n 4.
[49] Arner et al., *op cit.* n 25.
[50] *Ibid*.
[51] Bharadwaj, *op. cit.* n 4.
[52] Arner et al., *op cit.* n 25.
[53] Bharadwaj, *op. cit.* n 4.
[54] *Ibid*.
[55] S Ga, D Xu, H Wang, and Y Wang, *Intelligent Anti-Money Laundering System*, 2006 IEEE International Conference on Service Operations and Logistics, and Informatics (2006).
[56] *Ibid*.
[57] T Dutton, "An Overview of National AI Strategies", Medium, available at https://medium.com/politics-ai/an-overview-of-national-ai-strategies-2a70ec6edfd (accessed 23 January 2020).
[58] A Atabekov, O Yastrebov, "Legal Status of Artificial Intelligence Across Countries: Legislation on the Move", (2018) XXI *European Research Studies Journal* Issue 4, 773–782.
[59] *Notice of the State Council Issuing the New Generation of Artificial Intelligence Development Plan*, State Council Document [2017] No. 35.
[60] "National Strategy for Artificial Intelligence #AIFORAL", https://www.niti.gov.in/writereaddata/files/document_publication/NationalStrategy-for-AI-Discussion-Paper.pdf (last accessed 29 September, 2019).
[61] Executive Order on Maintaining American Leadership in Artificial Intelligence. That boat may have sailed as China seem to be the leader in this regard.
[62] M Murgia, S Shrikanth, "How Governments are Beginning to Regulating AI" "https://www.ft.com/content/025315e8-7e4d-11e9-81d2-f785092ab560 (published 30 May 2019) (Last accessed 29 September, 2019).
[63] "Recommendation of the Council on Artificial Intelligence" (published May 2019) https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449 (last accessed 29 September, 2019).
[64] https://www.g20trade-digital.go.jp/dl/Ministerial_Statement_on_Trade_and_Digital_Economy.pdf.
[65] "Artificial Intelligence: Commission Takes Forward its Work on Ethics Guideline", https://europa.eu/rapid/press-release_IP-19-1893_en.htm?locale=en (Published 8 April, 2019) (last accessed 29 September, 2019).
[66] AF Winfield and M Jirotka, "The Case for an Ethical Black Box," in *Towards Autonomous Robot Systems*, ed. Y Gao (Springer 2017), 1–12. Available at: http://eprints.uwe.ac.uk/31760.
[67] http://ai-elsi.org/wp-content/uploads/2017/05/JSAI-Ethical-Guidelines-1.pdf.
[68] US Senate Intelligence Committee Vice Chairman, Potential Policy Proposals for Regulation of Social Media and Technology Firms https://www.warner.senate.gov/public/_cache/files/d/3/d32c2f17-cc76-4e11-8aa9-897eb3c90d16/65A7C5D983F899DAAE5AA21F57BAD944.social-media-regulation-proposals.pdf.
[69] https://gdpr-info.eu/art-22-gdpr/
[70] See Michael Lewis, *Flash Boys* (W. W. Norton & Company 2015).
[71] It is important to understand the different kinds of AI: See R Martinez, "Artificial Intelligence: Distinguishing between Types & Definitions," (Spring 2019) 19 *Nevada Law Journal* no 3, 1015–1042.
[72] See report: *Artificial intelligence and National Security*, Congressional Research Service (updated 30 January, 2019) https://crsreports.congress.gov (R45178).
[73] See M Guihot; AF Matthew; NP Suzor, "Nudging Robots: Innovative Solutions to Regulate Artificial Intelligence", (Winter 2017) 20 *Vanderbilt Journal of Entertainment & Technology Law* no 2, 385–456. The authors provide a mature and deep discussion of the strategies that can be adopted to regulate AI given the information asymmetry an the inherent tensions presented.
[74] See M Joshi, "AI Tames the Complexity of Regulation in Financial Services" (2017) *Infosys Insight*, https://www.infosys.com/insights/ai-automation/Pages/AI-tames-complexity.aspx (last accessed 29 September 2019)
[75] China's success at AI has relied on good data, *The Economist*, Jan 2nd 2020 edition https://www.economist.com/technology-quarterly/2020/01/02/chinas-success-at-ai-has-relied-on-good-data.
[76] S Markose, S Giansante, A Rais Shaghaghic, "Too Interconnected to Fail Financial Network of US CDS Market: Topological Fragility and Systemic Risk", (August 2012) 83 *Journal of Economic Behavior & Organization*, no 3, 627–646.
[77] DW Arner, J Barberis, and RP Buckley, "FinTech, RegTech, and the Reconceptualization of Financial Regulation", (2017) 37 *Nw. J. Int'l L. & Bus.* 371, http://scholarlycommons.law.northwestern.edu/njilb/vol37/iss3/2.
[78] There is a significant body of literature on the implication of machine generated output on the law of intellectual property. Fundamentally, scholars have for years now attempted to address the questions of ownership rights and IP protection in regard to AI generated materials.
[79] See Y-T Wu, "FinTech Innovation and Anti-Money Laundering Compliance", (September 2017) 12 *National Taiwan University Law Review* no 2, 201–258.
[80] See DW Arner, J Barberis, RP Buckey, "FinTech, RegTech, and the Reconceptualization of Financial Regulation", (Summer 2017) 37 *Northwestern Journal of International Law & Business* no 3, 371–414; See also, DW Arner, DA Zetzsche,

RP Buckley, JN Barberis, "FinTech and RegTech: Enabling Innovation While Preserving Financial Stability", (Fall 2017) 18 *Georgetown Journal of International Affairs* no 3, 47–58

[81] See CA Tschider, "Regulating the Internet of Things: Discrimination, Privacy, and Cybersecurity in the Artificial Intelligence Age", (2018) 96 *Denver Law Review* no 1, 87–144, 98; see additional data risks in DA Zetzsche, DW Arner, RP Buckley, and B Tang, "Artificial Intelligence in Finance: Putting the Human in the Loop", (February 2020). CFTE Academic Paper Series: Centre for Finance, Technology and Entrepreneurship, no. 1. Available at SSRN: https://ssrn.com/abstract= at p.18.

[82] Not just in the context of financial services but more generally. Specific Anti-discrimination legislation with respect to the financial sector does however exist: See *Equal Credit Opportunity Act* (ECOA) (codified at 15 U.S.C. § 1691 et seq.).

[83] See, for example in relation to AI-influenced hiring practices, MJ Girouard, "Big Data, Bigger Risk: Recognizing and Managing the Perils of Using Algorithms in Recruiting and Hiring", (July–August 2019) 2 *RAIL: The Journal of Robotics, Artificial Intelligence & Law*, no 4, 235–242.

[84] HKMA and PwC, "Reshaping Banking with Artificial Intelligence", (2019), https://www.hkma.gov.hk/media/eng/doc/key-functions/finanical-infrastructure/Whitepaper_on_AI.pdf.

[85] J Truby, "Governing Artificial Intelligence to benefit the UN Sustainable Development Goals", (2020) *Sustainable Development*.

[86] *Ibid*.

[87] Hillman, "The Use of Artificial Intelligence in Gauging the Risk of Recidivism", (2019) 58 *The Judges Journal* 40; Machine bias, J Angwin, J Larson, S Mattu, L Kirchner – ProPublica, May, 2016.

[88] Minority Neighborhoods Pay Higher Car Insurance Premiums Than White Areas With the Same Risk – J Angwin, J Larson, L Kirchner, S Mattu – ProPublica, April, 2017.

[89] On an intellectual level, if humans were to artificially hamstring AI in preventing the system from optimal development based purely on its internal logic – are not the benefits of AI essentially cancelled out?

[90] Again this is one of the OECD principles.

[91] The issue of AI liability is one of the oldest topics in the body of literature focused on AI and Law. See GS Cole, "Tort Liability for Artificial Intelligence and Expert Systems", (April 1990) 10 *Computer/Law Journal* no 2, 127–232; ME Gerstner, "Liability Issues with Artificial Intelligence Software", (1993) 33 *Santa Clara Law Review* no 1, 239–270; OE Radutniy, "Criminal Liability of the Artificial Intelligence", (2017) 138 *Problems of Legality* 132–141.

[92] W Kowert, "The Foreseeability of Human-Artificial Intelligence Interactions", *Texas Law Review* 96 *Tex. L. Rev.* 181.

[93] SEC Charges Two Robo-Advisers With False Disclosures (published 21 December, 2018) (last accessed 29 September, 2019).

[94] Who to Sue When a Robot Loses Your Fortune, Bloomberg, 6 May 2019, https://www.bloomberg.com/news/articles/2019-05-06/who-to-sue-when-a-robot-loses-your-fortune (last accessed 12 December, 2019).

[95] See CA Tschider, "Regulating the Internet of Things: Discrimination, Privacy, and Cybersecurity in the Artificial Intelligence Age", (2018) 96 *Denver Law Review* no 1, 87–144, 138.

[96] 15 U.S.C. § 1681.

[97] GDPR, Article 17, also creates a right to have data deleted, which could have implications for the extent of data that can be discovered by an algorithm.

[98] GDPR, Article 22. https://gdpr-info.eu/art-22-gdpr/ (last accessed 29 September, 2019).

[99] GDPR, Article 22 (2). https://gdpr-info.eu/art-22-gdpr/ (last accessed 29 September, 2019).

[100] SJ Moore, "Artificial Intelligence in the Workplace", (November/December 2017) 31 *Ohio Lawyer* no 6, 18–20, 20.

[101] Given the advances in AI technology, the use of extensive voice samples to create systems that can mimic the original voice is startling. The technical ability to overlay that voice on a video is even more frightening: See S Suwajanakorn, "Fake Videos are Real: And How to Spot Them", https://www.ted.com/talks/supasorn_suwajanakorn_fake_videos_of_real_people_and_how_to_spot_them/transcript?language=en (last accessed 29 September, 2019).

[102] For example, a financial advisor may be required to answer for a conflict of interest of which they are unaware. A strong AI system may discover that a financial advisor has an indirect (and distant) interest in the subject matter being recommended to a client. Share ownership in pension funds and other complex financial relations discernable only to the AI system may trigger flags when in reality the indirect interest of the advisor are playing no part in the advice process because they are so remote. The time and energy required to sort through such scenarios is a deadweight loss to the economy.