The current issue and full text archive of this journal is available on Emerald Insight at:
https://www.emerald.com/insight/1359-0790.htm

Artificial intelligence and deep learning: considerations for financial institutions for compliance with the regulatory burden in the United Kingdom

Charanjit Singh
Holborn Chambers, London, UK and University of Westminster, London, UK

Abstract

Purpose – Artificial intelligence (AI), machine learning (ML) and deep learning (DL) are having a major impact on banking (FinTech), health (HealthTech), law (RegTech) and other sectors such as charitable fundraising (CharityTech). The pace of technological innovation and the ability of AI systems to think like human beings (simulate human intelligence), perform tasks independently, develop intelligence based on its own experiences and process layers of information to learn ever-complex representations of data (ML/DL) means that improvements in the rates at which this technology can undertake complex, technical and time-consuming tasks, identify people, objects, voices, patterns, etc., screen for 'problems' earlier, and provide solutions, provide astounding benefit in economic, political and social terms. The purpose of this paper is to explore advents in AI, ML and DL in the context of the regulatory compliance challenge faced by financial institutions in the United Kingdom (UK).

Design/methodology/approach – The subject is explored through the analysis of data and domestic and international published literature. The first part of the paper summarises the context of current regulatory issues, the advents in deep learning, how financial institutions are currently using AI, and how AI could provide further technological solutions to regulatory compliance as of February 2023.

Findings – It is suggested that UK financial institutions can further utilise AI, ML and DL as part of an armoury of solutions that ease the regulatory burden and achieve high levels of compliance success.

Originality/value – To the best of the author's knowledge, this is the first study to specifically explore how AI, ML and DL can continue to assist UK financial institutions in meeting the regulatory compliance challenge and the opportunities provided for financial institutions by the metaverse.

Keywords RegTech, Regulation, Deep learning, Machine learning, Artificial intelligence, English law

Paper type Research paper

1. Introduction

Artificial intelligence (AI), machine learning (ML) and deep learning (DL) are changing the way in which organisations work. The rate of technological innovation and the ability of AI systems to think like human-beings (simulate human intelligence), perform tasks independently, develop intelligence based on its own experiences and process layers of information to learn

All persons who meet authorship criteria are listed as authors, and all authors certify that they have participated sufficiently in the work to take public responsibility for the content, including participation in the concept, design, analysis, writing, or revision of the manuscript.

Furthermore, the author certifies that this material or similar material has not been and will not be submitted to or published in any other publication before its appearance.

Journal of Financial Crime
© Emerald Publishing Limited
1359-0790
DOI 10.1108/JFC-01-2023-0011

ever-complex representations of data (ML/DL) means that improvements in the rates at which this technology can undertake complex, technical, tedious and time-consuming tasks, identify people, objects, voices, patterns, etc., screen for "problems" earlier, and provide solutions, provide astounding benefit in economic, political and social terms. Thus, AI, ML and DL have become buzzwords or colloquialisms that are often used synonymously, albeit all three mean different things, the potential of which is now engrained intimately into the fabric of technology systems as governments, organisations and even regulators seek to benefit from the innovative solutions that they offer.

The purpose of this article is to explore advents in AI, ML and DL in the context of the financial institutions and the regulatory compliance challenge they face in the United Kingdom (UK). This article explores how AI, ML and DL can, as a RegTech tool, assist these organisations in tackling that issue. In so doing, it is investigated what AI, ML and DL can assist with as trustworthy components in the arsenal of financial institutions in assisting regulatory compliance (Singh *et al.*, 2020).

2. Practical considerations and "costs"

Financial institutions, in England and Wales, are regulated organisations subject to the Financial Services Act 2012 that paved the way for a tripart regulator system comprising of the Financial Conduct Authority (FCA), the Prudential Regulatory Authority (PRA) and the Financial Planning Committee (FPC). Whilst a discussion of their functions, and those of collateral bodies such as the Financial Reporting Council and Financial Ombudsman Service, is beyond the scope of this article, it is salient to provide a brief statistical snapshot to give context to the magnitude of the regulatory compliance task at hand [1]. The FCA is tasked with ensuring that the financial market is honest, fair and effective – for businesses, the economy and consumers. It seeks to ensure that consumers get a fair deal. The FCA regulates the conduct of over 50,000 businesses, prudentially supervises 48,000 organisations and sets specific standards for 18,000 firms. The PRA regulates over 1,500 banks, building societies, credit unions, insurers and large investment firms, and the FPC leads the Bank of England's work on financial stability by identifying and monitoring risks that may threaten the resilience of the UK's entire financial system. Thus, whilst the PRA focuses on individual firms, in contrast, FPC concentrates on the whole system.

Regulators all have rules and guidance that must be followed, and financial services are no different. In addition to the rules and codes set by the regulators, cybercrime, anti-money laundering, counter-terror finance and fraud are all matters that affect financial institutions, and there are extensive legislative regimes that must be adhered to. What follows is a brief summary that will help contextualise the size of the regulatory compliance task/burden.

2.1 The current legislative regime and industry guidance and standards

The main UK sources of law that regulate financial crime and that financial institutions must be aware of and/or comply with are:

- Proceeds of Crime Act 2002 (POCA, money laundering).
- Terrorism Act 2000 (TA, terror finance).
- Anti-Terrorism, Crime and Security Act 2001 (powers against terror assets i.e. seizure and power to freeze).
- Criminal Finances Act 2017 (CFA provides powers to recover proceeds of crime, tax evasion and corruption, as well as terrorism).

- Economic Crime (Transparency and Enforcement) Act 2022 (ECTEA focuses on Russian dirty money and investigation of illicit wealth – note passed by effect of the Ukraine War).
- Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 (MLRs, requirements on regulated firms to contact ML and TF, also determine identity of customers, transaction purposes and source of funds, etc.).
- Sanctions and Anti-Money Laundering Act 2018 (AAMLA relates to the implementation of international sanctions regimes, etc.).
- Serious Crime Act 2015 (SCA helps bring serious and organised criminals to justice by building on civil and criminal law).

Financial institutions also follow, amongst others, these industry standards and guidance:

- BSI PAS 17271 Code of Practice.
- CRM Code – Lending Standards Board.
- FCA Sourcebook of Rules and Guidance including the Senior Management Arrangements, Systems and Controls Handbook (SYSC).
- Financial Action Task Force (FATF) Recommendations.
- Financial Crime – A Guide for Firms.
- His Majesty's Treasury's, Treasury Advisory Notes.
- Joint Money Laundering Steering Group (JMLSG) Guidance for UK Financial Sector on the prevent of ML and TF.
- UK National Risk Assessment of ML and TF.

2.2 The economic crime and corporate transparency bill

This bill seeks to build on the Economic Crime (Transparency and Enforcement) Act 2022 and focuses its attention on criminals, kleptocrats and terrorists; it seeks to drive "dirty money" out of the UK financial system. The bill introduces reform to Companies House to prevent abuse of partnerships, provides a more efficient framework for the seizure of crypto-assets, and seeks to promote targeted information sharing, further powers to gather intelligence but also removes regulatory burdens on business.

2.3 Cost of financial crime

The exact cost of financial (or economic) crime is unknown, but the figure for the UK alone from corruption, fraud and money laundering is likely to run into billions of pounds each year, and it is estimated such criminality is equivalent to 3.6% of global GDP (Cregg, 2022; Reichel, 2019; Walker *et al.*, 2006). London is "the" preferred "laundromat" for Russian ill-gotten gains [2], and therefore, financial institutions are seen to be particularly vulnerable. Globally, the level of financial crime has remained stable. Price Waterhouse Cooper's Global Economic Crime and Fraud Survey (2022) revealed that 46% of the firms they work with across 99 territories experienced some form of financial crime, with cybercrime posing the greatest challenge (Price Waterhouse Coopers, 2022). The European Commission estimated that the global cost of just "cybercrime" in 2020 was circa €5.5tn [3]. Therefore, the cost of compliance is high, but non-compliance could be substantially higher encumbering penalties in the form of fines, regulatory actions and losses to financial institutions and their customers, as well as reputational damage causing further loss of custom (see FICO, 2022) [4]. Globally, institutions were fined huge sums and that is just for anti-money laundering breaches: €5.6bn during the period 2015–2021 and €2.5bn in 2021 alone, the average fine was €31.79mn (Fraugster, 2022), and thus, these factors give impetus for improvement. One mechanism to do that would be through AI, ML and DL.

3. Artificial intelligence, machine learning and deep learning

AI has already proven its benefits in achieving low human resource costs and high levels of accuracy and speed. This frees up time for high levels of business and relationship-building and other direct profit-generating activities. In short, AI, of which ML is a constituent technology and of which DL is a subset, allows a machine or series of machines to act, comprehend, experience, learn and sense just like their human counterparts but far more efficiently. In numerical terms, AI is thousands of times faster than human beings, and unsurprisingly, it will outperform them in all tasks by 2060 (Revell, 2023; Carrigan and Porpora, 2023), from driving transport right through to performing complex surgical procedures. AI and ML were discussed in depth in earlier articles (Singh *et al.*, 2022, 2021, 2020).

Deep learning (DL) is a constituent of AI and a form or subset of ML in which the system is trained to identify patterns in i.e. pictures, sounds, text or other datasets and accurately predict or provide insight. DL can be used to automate tasks such as voice-to-text or picture description, process natural language, classify images, intelligent analysis of long form documentation and analysing speech. DL is becoming more popular and is widely used in fraud detection, chat boxes, facial recognition, to generate subtitles for social media videos on YouTube or in Panopto for educational purposes, and in digital assistants such as Microsoft's Cortana (Li, 2017), Apple's Siri or Amazon's Alexa. DL can be used to track activity and create "personalised" experiences, recommendations and services. It should also be noted that access to that "data" is regulated by a range of legislation including the General Data Protection Regulation 2016/679 (GDPR) (see recital 30 regarding online identifiers; note also: s.3 of the European Withdraw Act 2018 for the purposes of the UK). The monitoring and/or use of data or browsing data (cookies) is subject to curtailment, which is not surprising given the misuse of user information in a series of scandals involving companies such as Facebook (now Meta) and the defunct Cambridge Analytica [5]. But, in general, sharing is still quite extensive.

DL algorithms (DLAs) are artificial neural networks (AN) based on the human brain; artificial neurons are nodes (software modules) that use mathematical calculations to process data. DLAs use the nodes to solve complex or technical problems. There are three components to a deep neural network: the "input" layer, "hidden" layer and "output" layer. The AN will have many nodes that input the data into it, the hidden layer then processes the data at various levels and changes its behaviour as it receives further tranches of data; therefore, DL is experiential (Goodfellow *et al.*, 2017). There are often several hundred hidden layers, and therefore, the problem is analysed from a variety of perspectives. For example, from an image, each layer may analyse a different feature from it. The output layer then provides the answer, which can be affirmative, negative (two nodes) or far more sophisticated.

There are benefits and challenges of using DL over traditional ML, some of these are:

- Data that unstructured is processed more easily.
- Deep analysis of large amounts of complex data can reveal new perspectives, ones that the algorithm may not have been trained for.
- It learns from user behaviour (unsupervised learning); therefore, it is experiential.

- It is efficient where the categorisation and analysis of volatile data is concerned, which can assist in better fraud prevention and detection.
- The results are improved when the DLA is trained on high-quality datasets. Therefore, the dataset must be "cleaned" before the DLA is trained.
- Large data storage capacity for input data pre-processing is needed, as well as sufficient capacity to compute that (infrastructure), otherwise results are slower.

Overall, the benefits outweigh the challenges when compared to traditional ML methods.

4. Financial institutions and their use of DL – current advents and forthcoming trends

4.1 Current DL use in financial institutions

Financial institutions are using AI to interact with customers; DL is being used to furnish customers with natural feeling and personal interactive experiences and real-time problem solving, but use is still relatively conservative. AI is allowing financial institutions to enhance customer experience while also streamlining their operations to harness better support and enhanced security with smoother processing. Generally, AI is being used for:

- credit scoring;
- customer retention;
- digital on-boarding and document processing;
- fraud detection;
- investing;
- payments; and
- regulatory compliance.

This has resulted in savings in time, cost and risk (operational) and provides real-time fraud detection by skimming through vast quantities of data with relative ease. Regulatory compliance is resource intensive; many financial institutions spend millions of pounds on trying to achieve this, but even then, they may fall victim to criminality and/or breach the rules. Thus, DL is more beneficial as a RegTech tool than traditional ML because of its learning abilities, and thus, it can be more easily used to process machine-readable documentation published by regulators, to recognise differences and correlations between the rules and to provide updates. DL can monitor regulatory changes and implement those whilst disseminating information to those front-line workers who need it i.e. compliance professionals or lawyers. DL can also help financial institutions monitor customer behaviour and transaction data to detect and prevent financial crimes, such as fraud, money laundering and financing of terrorism, and ensure that all transactions comply with the relevant regulatory requirements and/or are flagged-up or reported. At the very least, DL should be used to automate error-prone workflows such as data entry, etc. [6]. Thus, the most common operational matters that are suitable for further DL intervention/automation include:

- information centric processes: reduce manual data processing;
- E-customer due diligence and e-know your customer;
- databases to share CDD and KYC information;
- audit, identify, track and trace, and report functions;

- link analysis – beneficial ownership;
- policy updates, machine readable and executable documentation;
- creation of training materials;
- stakeholder interaction;
- sanctions regime compliance; and
- linguistic data analysis – to enhance fraud detection, etc.

This would result in substantial inroads being made into curtailing consistent compliance failures.

4.2 The metaverse

The "metaverse" (Hackl *et al.*, 2022; QuHarrison *et al.*, 2022) is the current buzzword within financial institutions, it is in short digital spaces that are decentralised, incorporate augmented and virtual reality, store information on blockchain technology where consumers can own digital goods. For financial institutions, this means potentially *new markets and products*. Hackl *et al.* (2022) argue that the metaverse poses three paradigmatic shifts in terms of the internet or what it means to be "online", these are:

- Experience: People do not just want to consume. It is far more engaging to have gamified, contextual experiences.
- Identity: People value their digital persona and want to carry it with them across the metaverse and even into the real world.
- Ownership: Wherever people choose to spend their time, they want skin in the game [7].

The metaverse relies on AI and presents opportunities in terms of business-and-consumer collaboration; customers can attend events or even receive financial planning and advice from a digital representative (avatar). It is believed that in the future, most customers will consume services in the real world, online (internet) and in the metaverse. Advents in financial products include *insurance for tangible and intangible property, cryptocurrency*, etc. Thus, customers will spend real money (currency) plus digital money both online and offline. This also provides impetus for financial institutions to begin to engage further with AI, most notably the benefits of DL.

5. Conclusion

Regulators in the financial services industry are actively engaging with AI, and thus, institutions should also harness the progress made by them, the technology and the RegTech revolution. There is an opportunity to further reduce the occurrence of compliance breaches and crime by expanding the use of DL, where AI can help in the conduct of business. To be fair, the finance sector has grasped many digital and technological transformation initiatives unlike others, such as charities, but a lot more can be done. AI can assist institutions in cutting operational costs, promoting greater levels of regulatory compliance and building stronger relationships based on trust and confidence with stakeholders. Expanding analytical tools and automating processes can assist institutions in reducing risk and successfully fighting financial crime. Finally, the financial services industry needs to further engage with the metaverse so that they can harness the manifold opportunities it offers for new experiences, products and services.

Notes

1. For a breakdown of the FCA figures, see: www.fca.org.uk/about. Facts in relation to the PRA and FPC are available on: www.bankofengland.co.uk/
2. *Russia Report. Intelligence and Security Committee of Parliament.* UK: HMSO. See: https://isc.independent.gov.uk/wp-content/uploads/2021/03/CCS207_CCS0221966010-001_Russia-Report-v02-Web_Accessible.pdf
3. European Commission. *A cybersecure digital transformation in a complex threat environment.* Brochure. Brussels, 28 January 2021.
4. *Consumer Survey 2022: Fraud, identity, and digital banking in the UK.* (2022). UK: FICO. See, www.fico.com/es/latest-thinking/ebook/consumer-survey-2022-fraud-identity-and-digital-banking-uk
5. *Facebook agrees to pay UK fine over Cambridge Analytica scandal.* Reuters, 30 October 2019. See, www.reuters.com/article/us-facebook-privacy-britain-idUSKBN1X913O. See also, *Investigation into the use of data analytics in political campaigns: A report to Parliament.* Information Commissioners Office, 6 November 2018. UK: HMSO.
6. In terms of bias and AI see, Bellamy, R. K. E. et al. *AI Fairness 360: An extensible toolkit for detecting and mitigating algorithmic bias.* IBM Journal of Research and Development, vol. 63, no. 4/5, pp. 4:1-4:15, 1 July-Sept. 2019. Also see the AI resource centre: IBM. *Mitigating Human Bias in AI.* 2020. See, www.research.ibm.com/5-in-5/ai-and-bias/. Also: Wood, J. *This AI outperformed 20 corporate lawyers at legal work.* World Economic Forum 2020. See, www.weforum.org/agenda/2018/11/this-ai-outperformed-20-corporate-lawyers-at-legal-work/
7. Hackl *et al.* (2022) in: Stackpole, T. Exploring the Metaverse. HBR, July – August 2022. See, https://hbr.org/2022/07/exploring-the-metaverse

References

Carrigan, M. and Porpora, D. (Eds) (2023), *Post-Human Futures: Human Enhancement, Artificial Intelligence and Social Theory (the Future of the Human)*, Routledge, London.

Cregg, P. (2022) "How can banks address the rising financial crime rate?", FinTech Magazine, available at: https://fintechmagazine.com/banking/how-can-banks-address-the-rising-financial-crime-rate

Fraugster (2022), "Payment intelligence report", UK, Fraugster, available at: https://resources.fraugster.com/hubfs/Fraugsters%20Payment%20Intelligence%20Report%202022.pdf

Goodfellow, I., Bengio, Y., Courville, A. and Bach, F. (2017), *Deep Learning (Adaptive Computation and Machine Learning Series)*, MIT Press, London.

Hackl, C., *et al.* (2022), *Navigating the Metaverse: A Guide to Limitless Possibilities in a Web 3.0 World*, Wiley, New Jersey.

Li, J. (2017), *Deep Learning Acoustic Model in Microsoft Cortana Voice Assistant*, AI and Research, Microsoft.

Price Waterhouse Coopers (2022), "PwC's global economic crime and fraud survey", available at: www.pwc.com/gx/en/forensics/gecsm-2022/pdf/PwC's-Global-Economic-Crime-and-Fraud-Survey-2022.pdf

QuHarrison, T., *et al.* (2022), *The Metaverse Handbook: Innovating for the Internet's Next Tectonic Shift*, Wiley, New Jersey.

Reichel, P. (2019), *Global Crime: An Encyclopaedia of Cyber Theft, Weapons Sales, and Other Illegal Activities*, Greenwood Press pp. 148-154.

Revell, T. (2023), "AI will be able to beat us at everything by 2060", The New Scientist 2017, available at: www.newscientist.com/article/2133188-ai-will-be-able-to-beat-us-at-everything-by-2060-say-experts/

Singh, C., *et al.* (2020), "Can artificial intelligence, RegTech and CharityTech provide effective solutions for anti-money laundering and counter-terror financing initiatives in charitable fundraising", *Journal of Money Laundering Control*, Vol. 24 No. 3, pp. 464-482, doi: 10.1108/JMLC-09-2020-0100.

Singh, C., *et al.* (2021), "Can machine learning, as a RegTech compliance tool, lighten the regulatory burden for charitable organisations in the United Kingdom?", *Journal of Financial Crime*, Vol. 29 No. 1, pp. 45-61.

Singh, C., *et al.* (2022), *RegTech Compliance Tools for Charities in the United Kingdom: Can Machine Learning Help Lighten the Regulatory Burden*?, The Company Lawyer, Sweet and Maxwell.

Walker, D., Brock, S. and Ramon, T. (2006), "Faceless orientated policing: traditional policing theories are not adequate in a cyber world", *The Police Journal: Theory, Practice and Principles*, Vol. 79 No. 2, pp. 169-309.

About the author

Charanjit Singh, Tenant and Barrister-at-Law, Holborn Chambers and Assistant Head of School, University of Westminster, and PhD – University of Southampton. Charanjit Singh can be contacted at: c.Singh1@westminster.ac.uk