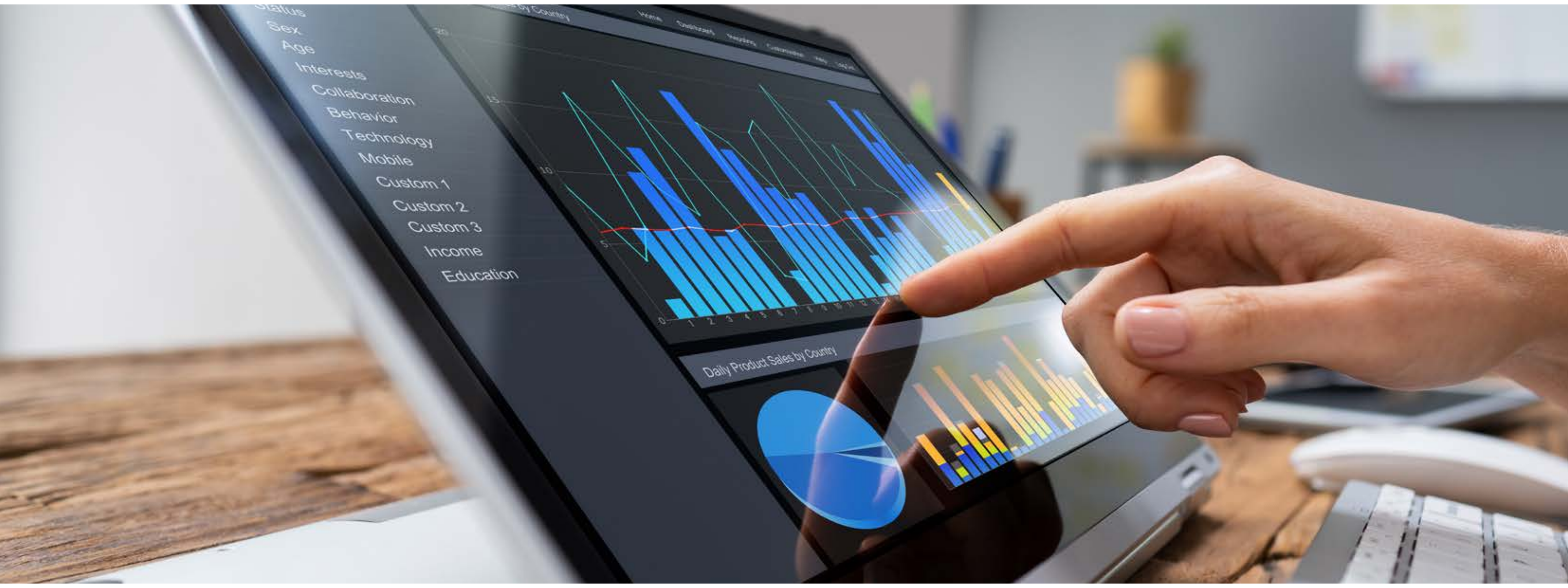
ALLEN & OVERY

Artificial Intelligence in insurance – innovating in a world of increased regulation

Charlotte Rowlandson



The potential benefits of deploying artificial intelligence (**AI**) (and in particular, *machine learning* (**ML**) techniques) within the insurance industry have been the subject of much market discussion and increased focus over recent years. Whereas attention was initially turned towards retail fraud detection software, clear use cases are now emerging throughout the insurance value chain across consumer and commercial lines, with the potential to improve the customer experience, facilitate better underwriting and portfolio risk management and create efficiencies in back-office operations.

While *AI* use cases currently in live, widespread deployment within the insurance industry remain (for the most part) relatively simple in nature, board level interest in, and the rate of adoption of, *AI* is increasing. Most incumbent firms have begun to dip a proverbial toe into the water of *AI*, with a view to identifying the "low hanging fruit" (in terms of deploying *AI* to maximise efficiency gains in areas of perceived lower regulatory risk) while they seek to understand the underlying technologies and their significant implications for operating insurance business in the future. Against this backdrop, the potential for regulatory lag has emerged in relation to the approach to the regulation of *AI* and the extent to which existing regulatory frameworks remain fit for purpose in the context of these developing technologies.

This note provides an overview of the status of adoption of *AI* within the insurance industry and the potential legal, regulatory and commercial challenges this exciting technology represents. It also draws from guidance published by financial services regulators to date to provide practical guidance to firms to identify features that may represent a heightened risk profile as use cases become increasingly complex, and develop risk mitigation strategies to assist those operating in this space to navigate the regulatory uncertainty, so as to facilitate innovation and expedite the adoption of *AI* within the sector.

A useful glossary of italicised technical terms used in this note can be found in the Alan Turing Institute paper on "AI in Financial Services".

How is *AI* being deployed within the insurance industry?

In its paper on "AI in Financial Services" commissioned by the UK Financial Conduct Authority, the Alan Turing Institute identified three key areas of recent innovation that have combined to facilitate the acceleration in deployment of *AI* within the financial services sector:

- ***ML*** – developments in the field of *ML* (including deep learning, a higher complexity subset of *ML*), which have also been combined with other *AI* techniques (such as *natural language processing*)
- **expanding data sets** – increased data collection (both in terms of volume and number of *non-traditional data* points collected) through the expansion of the internet of things, which (importantly) is undertaken in a structured format that can then be subjected to data analytics
- ***automation*** – developments in technologies enabling the automation of high volume, resource intensive processes previously undertaken by humans.

EIOPA's paper "Artificial Intelligence Governance Principles: towards Ethical and Trustworthy Artificial Intelligence in the European Insurance Sector" outlined its findings on the proliferation of the use of *AI* across all parts of the insurance value chain, alongside anticipated *AI* use cases within the insurance industry and associated areas of regulatory concern. Key amongst these is the use of *AI* in underwriting and pricing, portfolio risk management across the existing book and on the retail side in particular, claims notification and fraud detection.

Given the anticipated significance of the application of *ML* to activities within the insurance value chain, the majority of the discussion in this note refers principally to *AI* use cases incorporating *ML* techniques.

Legal, regulatory and commercial challenges

There are various well documented legal, regulatory and commercial pitfalls when it comes to deploying *AI* in insurance settings. While many regulatory bodies worldwide have been specifically tasked with facilitating technological innovation within their respective spheres and certain jurisdictions (including the UK) have adopted national strategies for the growth of AI development, there is a clear acknowledgment that existing legal and regulatory frameworks will likely need to be revisited and adapted to address the potential risks and harms arising from the application of *AI* within financial services (and beyond).

In order to meet these competing objectives, regulators will need to address certain gating questions arising in relation to the regulation of *AI*, which (in of themselves) reflect the multi-faceted legal and regulatory risks posed and underline the complexity of the challenge faced by regulators:

- **the scope of the term "artificial intelligence"** – *AI* is an evolving field of computer science with complex concepts that are continually developing. This gives rise to an initial, significant challenge simply in terms of defining the scope of computational and mathematical methodologies using innovative data analytics and data modelling techniques that should fall within "artificial intelligence" for the purposes of relevant regulatory frameworks. While precision lends itself to clarity in interpretation and application, it also gives rise to significant risk of failing to keep pace with technological developments and a likely requirement for constant revision and expansion (with the associated potential to stifle innovation through uncertainty). Conversely, if the definition is too "broad brush" it may not strike an appropriate balance in relation to proportionate and targeted, risk-based regulation.
- **regulatory approach** – *AI* is currently governed by a patchwork of laws, regulations and regulatory guidance. Governments and regulators will need to determine how best to approach the regulation of *AI*, for example, on a subject matter specific horizontal basis across all industries (akin to the approach taken by the EU in its General Data Protection Regulation and its proposal for the Artificial Intelligence Regulation (the ***Draft EU AI Reg***) or through sector specific rules (akin to the approach generally taken by regulators to financial services regulation). If the former approach is adopted, insurance regulators will be left to consider the extent to which existing financial services regulatory frameworks adequately address regulatory issues that have the potential to be exacerbated by the use of *ML*, for example, moral hazard issues arising due to diminishing risk pools and micro-risk segmentation as a result of the ability to analyse Big Data sets and underwrite on a more informed, data-driven basis. These risks will be particularly acute in retail lines, especially in relation to products analysing health and other sensitive personal data for underwriting purposes. Most existing financial services regulatory frameworks operate on a technology neutral basis and continue to be applicable to firms when adopting *AI* technologies, in particular in relation to the requirements under: (i) Solvency II for implementation of effective governance systems and high data quality (with "*accurate, complete and appropriate*" being the bedrock for successful data-driven supervision and evidence-based decision making as well as micro- and macro-prudential analysis); and (ii) the Insurance Distribution Directive, including potential limited access to, or exclusion from, financial products resulting from data-centric, highly individualised underwriting practices, ensuring that

products are aligned with the needs of the target market and acting honestly, fairly and professionally in accordance with the best interests of customers. In the UK, the implications of new Consumer Duty will also be relevant to the use of *AI* in the context of providing good outcomes for retail customers, including the extent to which disclosures and *system transparency* will be required in order to evidence compliance with the cross-cutting rules.

– **responsible regulator** – linked to the above, the legal and regulatory challenges posed by *AI* span across several regulatory spheres, notably data protection, competition, product standards, consumer protection and in the case of insurance and other financial products, financial services. This gives rise to a need for regulatory cooperation to avoid the significant potential for multiple, conflicting regulations arising, both within jurisdictions and globally.

In its July 2022 policy paper on "Establishing a pro-innovation approach to regulating AI", the UK government set out its intention to establish a set of non-statutory, cross-sectoral principles tailored to the distinct characteristics of *AI*, with regulators being asked to interpret, prioritise and implement these principles within their sectors and domains, all through a pro-innovation lens bearing in mind the importance of proportionality and adaptability. While this sounds great on paper, it is easy to see how challenging the task at hand is for the regulatory community. The scale of the task and the pace of technological development combined with the limited resources undoubtedly increases the scope for regulatory lag.

In the meantime, understanding, identifying and managing these legal, regulatory and commercial challenges will be critical for any industry participant developing or using (directly, or via its suppliers or subcontractors) *AI* (and in particular, *ML*) as part of its business, as well as any institutional investor evaluating opportunities within this space:

– **insurtechs** – it will be essential for insurtechs to ensure that the design and implementation of *AI* use cases comply with applicable legal and regulatory requirements in order for the business to operate within the highly regulated insurance industry and preserve its value proposition, regardless of whether the business model envisages servicing clients on a SaaS basis or operating as a neo-insurer/intermediary

– **incumbent insurers and intermediaries** – in view of the relatively nascent nature of *ML* techniques in particular, embarking on *AI* projects internally or as part of engagements with technology partners represents a heightened regulatory and reputational risk profile requiring consideration of nuances specific to the insurance industry and ongoing risk management

– **investors** – *AI* use cases will represent a key area of due diligence by investors seeking to validate the value proposition presented by a target. It will also be important to understand the extent to which legal and regulatory requirements impact on the commercial viability of a target's business model. By way of example, consider a business model that is reliant on the use of *ML* to analyse personal data from individuals for underwriting purposes; is there any value in an *AI* model built using that data if the necessary consents were not obtained at the time of collection and can individuals be incentivised to provide relevant consents so that business can utilise data collected to function going forward?

Risk assessment factors

However regulation in this space develops, proportionality will be the guiding principle. Indeed, in a statement delivered in February 2022 entitled "AI governance: Ensuring a trusted and financially inclusive insurance sector", EIOPA expressed support for the "*risk-based approach*" adopted by the European Commission in the Draft EU AI Reg, noting that "*not all AI systems pose the same opportunities and risks and hence the need for proportionality*". Similarly, the UK Prudential Regulation Authority noted in its October 2022 discussion paper on "Artificial Intelligence and Machine Learning" that "*a proportionate approach is critical to supporting the safe and responsible adoption of AI and other technologies across UK financial services*".

When embarking on a project or transaction involving the use of *AI* within the insurance industry (particularly those incorporating *ML* techniques), legal and compliance teams will need to be alive to features that may represent a heightened risk profile and necessitate a proportionately greater level of diligence and/or governance and monitoring.

While risk factors will be specific to individual use cases and should be assessed in the relevant context, considerations in relation to key areas of risk at the various stages of the *AI* lifecycle are set out below:

– ***AI supply chain*** (e.g. in circumstances where: (i) the development of an AI tool for use within an insurance business is being outsourced; (ii) insurance business activities are being outsourced to a third party provider that utilises AI tools; or (iii) insurance business activities are undertaken in-house using AI tools provided by a third party)

Tailored tools – is the *AI* specifically designed for the bespoke use case for which it is to be deployed (noting that where this is not the case, the *AI* tool is less likely to be appropriate for use in an insurance specific context)?

Third party suppliers – do any outsourcing arrangements comply with applicable regulatory outsourcing requirements? Where applicable, do the outsourcing agreements contain terms / rights required to be included under applicable law and regulation?

– ***system design***

ML approach – is the selected type of *ML* approach (e.g. *supervised learning, unsupervised learning or reinforcement learning*) appropriate for the analytical task in question? Have any trade-offs been made in relation to model complexity and opacity due to *inscrutability*? If so, are those trade-offs appropriate in the context of the *AI* use case and nature / level of risk posed?

Applicable laws – has the system design process contemplated whether any financial regulation, competition, data protection or equality frameworks or any specific frameworks relevant to *AI* technologies are relevant to the *AI* use case? Has the system design been developed with a view to complying with these requirements?

Training data – what data inputs are used to train the model and are they fit for purpose? Are they lawfully available (i.e. collected and held in compliance with applicable data protection and intellectual property requirements and contractual terms)? Are they accurate (noting that external data sources, whether privately contracted for or publically available, will likely represent a heightened level of risk)? Are there mechanisms in place for the identification of and protection against adversarial attacks through data poisoning (noting that this will be particularly relevant in relation to dynamic systems)? Is the data up-to-date (including, in relation to static machine learning models, consideration as to ongoing retraining requirements)? Is the data set complete (i.e. in the sense that sufficient data has been collected), conceptually valid (i.e. does the data set measure what it is assumed to measure) and representative (i.e. does the data set serve as a representation of the real world for the intended purpose)?

Human-in-the-loop (i.e. a human actively reviewing all decision making) or *human-on-the-loop* (i.e. ability for human supervision and intervention) – has a mechanism for human involvement been embedded within the system design? Is the level of human involvement (or lack thereof) appropriate in the context of the *AI* use case and nature / level of risk posed?

System transparency – can system logic information be interrogated through: (i) direct interpretation; or (ii) indirect interpretation using *explainability methods*? Is the approach acceptable for the purposes of complying with regulatory obligations? How is undesirable bias identified and mitigated?

Credit scoring – does the use case involve credit scoring, which is considered to give rise to a higher risk from a micro-risk segmentation / moral hazard perspective?

Retail business – is the use case anticipated to be deployed within a retail business context (which gives rise to a higher risk from a micro-risk segmentation / moral hazard / ESG perspective and likely gives rise to more acute data protection)?

– *system monitoring*

Communication of *system logic* – how is *system logic* information communicated? Would the format in which the system logic is communicated be intelligible to the average person?

Monitoring – how is user interaction and feedback monitored? Are there processes in place to identify over-reliance or undue distrust in the system? How quickly will software systems be updated following identification of any issues during monitoring processes?

Audit – what approach is taken to auditing system performance against design and deployment objectives? Who is responsible for undertaking audits? What is the frequency of audit cycles?

Audit validation – how are audit processes validated (for example, is this done through a self-certification process or are external auditors engaged for this purpose)? Is the approach appropriate?

– *system performance*

Training – what approach is taken to user training? Do users receive bespoke training based on their specific role in interacting with the relevant *AI* technologies?

Training updates – is the user training programme updated to reflect software updates / changes and to address any issues / risks identified as part of the monitoring processes?

Risk mitigation strategies

To the extent not already in place, firms should ensure that appropriate frameworks are implemented to both mitigate the risks arising from the development and deployment of *AI* within its insurance business and manage them in a proportionate manner. Risk mitigation strategies include:

– board / senior management oversight:

- board to receive training in relation to use of *AI* technologies within the business and the potential associated business continuity implications, regulatory and reputational risks in the event that issues arise. Board training should cover, for example, the types of *AI* technologies that are used, the processes in which the relevant types of *AI* technologies are used and the extent to which such processes are *AI* assisted (i.e. assists a human decision maker) or *AI* executed (i.e. no human intervention)
- overall responsibility for use of *AI* within the business to be designated to an individual manager (e.g. a specifically appointed "AI Officer"). In the UK, there is currently no dedicated senior management function (SMF) for AI, however for PRA-authorised SM&CR insurance firms and FCA-authorised enhanced scope SM&CR intermediaries, technology systems are the responsibility of the SMF24 (Chief Operations function) and overall management of risk controls is the responsibility of the SMF4 (Chief Risk function). The data protection officer and data protection function will also need to report into this overarching manager (noting that AI governance will be a cross-function responsibility).

– *internal governance frameworks* – internal governance frameworks and controls to be implemented covering:

- compliance with applicable legal and regulatory frameworks, including financial services regulatory, data protection, competition and *AI* specific regulations and ongoing monitoring of regulatory developments
- ethics, including data ethics protocols and addressing practices such as social scoring, exploitation of vulnerable groups and use of subliminal techniques
  and potentially also review by independent ethics oversight committees
- *AI* model selection, including decision making protocols in relation to making trade-offs between model complexity and opacity due to *inscrutability* in the context of the relevant use case
- user training requirements, including ongoing maintenance of training programmes
- record-keeping requirements, including requirements for records to be prepared and maintained documenting the relevant types of *AI* technologies deployed as part of use cases within the business, technical specifications, applicable monitoring regimes and system issues
- in relation to each *AI* system used or proposed to be used within the business, requirements for:
  - *AI* use case impact assessments to be undertaken, addressing the consideration set out under "Risk assessment factors" above
  - responsibility for system performance and compliance to be clearly allocated to designated individual(s) (whether to a single person or across multiple individuals by reference to risk area and / or different parts of the *AI* lifecycle), each of which will report into the individual manager with overall responsibility for use of AI within the business.

What next?

It would seem that, in parallel with the increasing adoption of *AI* by the insurance industry, there is a clear direction of travel from a political perspective in relation to its increased regulation, but also in support of innovation and adoption. Accordingly, we are likely to see further regulatory developments (whether by way of new legislation and regulations or regulatory guidance, including as to the applicability of existing laws and regulations in the context of *AI* technologies) released in the short to medium term. In the meantime, firms will need to ensure that innovation and investment in this area is undertaken alongside consideration of applicable legal and regulatory frameworks (including those in the pipeline) to ensure that areas of regulatory concern are addressed in a proportionate manner.

Meet the team

Philip Jarvis
Partner – London
Tel +44 20 3088 3381
philip.jarvis@allenovery.com

Kate McInerney
Partner – London
Tel +44 20 3088 4459
kate.mcinerney@allenovery.com

William Samengo-Turner
Partner – London
Tel +44 20 3088 4415
william.samengo-turner@allenovery.com

Charlotte Rowlandson
Senior Associate – London
Tel +44 20 3088 1104
charlotte.rowlandson@allenovery.com

Jane Finlayson-Brown
Partner – London
Tel +44 20 3088 3384
jane.finlayson-brown@allenovery.com

Karishma Brahmbhatt
Counsel – London
Tel +44 20 3088 2158
karishma.brahmbhatt@allenovery.com

Daren Orzechowski
Partner – Silicon Valley
Tel +1 650 388 1701
daren.orzechowski@allenovery.com

Allen & Overy means Allen & Overy LLP and/or its affiliated undertakings. Allen & Overy LLP is a limited liability partnership registered in England and Wales with registered number OC306763. Allen & Overy (Holdings) Limited is a limited company registered in England and Wales with registered number 07462870. Allen & Overy LLP and Allen & Overy (Holdings) Limited are authorised and regulated by the Solicitors Regulation Authority of England and Wales. The term partner is used to refer to a member of Allen & Overy LLP or a director of Allen & Overy (Holdings) Limited or, in either case, an employee or consultant with equivalent standing and qualifications or an individual with equivalent status in one of Allen & Overy LLP's affiliated undertakings. A list of the members of Allen & Overy LLP and of the non-members who are designated as partners, and a list of the directors of Allen & Overy (Holdings) Limited, is open to inspection at our registered office at One Bishops Square, London E1 6AD.