

Artificial Intelligence: regulatory approaches in the UAE and abroad



Artificial

Intelligence

Although there is a fair degree of debate as to what Artificial Intelligence (more commonly referred to as AI) is and what the term is mostly used to refer to, machines that incorporate some degree of human cognitive ability are not created equal and they range from simple recruitment applications and chatbot systems that possess 'machine learning' capabilities. The latter type is, as the name suggests, able to 'learn' on their own (using the data set fed into it) and thereby make accurate predictions and decisions. Some are even more complex and use 'deep learning' algorithms; i.e. algorithms that broadly mimic the information processing patterns found in the human brain, to make sense of new information they receive by comparing it to a known object.

Ridesharing apps like Uber and Careem use deep learning to calculate your route and trip fare; Tesla relies on a model of machine learning (that is not supervised by humans) to drive its auto-pilot features; and Netflix and Amazon use behavioural algorithms to predict which movies and television series you are likely to enjoy, and what products you are likely to be interested in based on your previous selections and purchases.

Although discourse on AI has been around for at least 60 years with numerous waves of development and excitement having each fizzled out, the field has taken the spotlight yet again more recently, except this time the latest wave of advances in AI promises to fundamentally change many aspects of our lives (more than the just the pure convenience factor brought about by the likes of Siri and Alexia). Consider for example, a use case of AI in the field of robotics which allows 68 billion dots binding DNA molecules to be imaged and 'read' in two minutes, thereby allowing every child to be tested for every possible genetic disease. All this and further progress (albeit at an accelerating pace) has been made possible as a result of the convergence of significantly faster, cheaper and on-demand (cloud based) computing processing power, coupled with an ever-increasing generation and availability of vast data sets (which AI systems rely

on to 'learn' and develop).

Should we regulate AI, and if so, how?

Safety and Liability

There is ongoing debate as to whether AI should be regulated and, if so, whether entirely new or separate legal systems and concepts would need to be developed (including whether new classes of liability that sit somewhere between personal liability and corporate liability should be created, and whether the burden of proof should be adapted or reversed) to address any safety issues posed by AI. Such risks may arise from defects in the AI system or code which result in, for example, an autonomous vehicle not recognising a pedestrian and as a result causing injury or death. Who should bear liability in such a case; the AI system driving the autonomous vehicle or the person who wrote the algorithm or code for the underlying software? Existing concepts such as reasonable foreseeability, intent and standard of care may not be appropriate for such systems which (at least for now) lack the entire spectrum of human cognitive ability and emotions.

Most regulators around the globe have thus far avoided implementing blanket AI regulations which cover all industries, for fear that such an approach may stifle innovation, particularly given the relative infancy of AI technology and its rapidly evolving nature. Although existing regulatory frameworks may not be entirely adequate to address novel risks inherent in AI, they provide a good foundation (at least for the level of AI that is generally available today) and can be amended and enhanced as appropriate to address AI specific risks. This approach has also been favoured by the UK House of Lords in its report titled '[AI in the UK: Ready, Willing, and Able](#)', as well as the European Union's recently released [White Paper on Artificial Intelligence](#), which among other things, sets out potential amendments and enhancements to existing EU legislation to address AI specific risks.

Industry specific regulations (such as the Abu Dhabi Department of Health's Policy on the Use of Artificial Intelligence in the Healthcare Sector) appear to be more appropriate as they present an agile and evidenced based approach to regulation, allowing specific risks to be addressed quickly without the unintended consequences inherent in more broad based law. As the pace of technological innovation increases exponentially and real risks (as opposed to theoretical ones) emerge, laws will need to continue to evolve (albeit much more quickly than we are accustomed to) and more industry specific regulations are likely to be enacted (or enhanced) as new AI use cases and associated risks crystallise.

It is worth noting that existing regulations, such as those relating to product liability, also indirectly apply to AI just as they would to any other product that malfunctions or is defective. Consider for example:

- Article 316 of the Civil Code which provides that '*any person who has things under his control which require special care in order to prevent their causing damage, or mechanical equipment, shall be liable for any harm done by such things or equipment...*'; and
- the Consumer Protection Law which prescribes penalties for (among other things) displaying, offering, promoting or advertising goods or services which cause damage to consumers, and, extends liability (by virtue of the definition of a 'provider') to the local agents and distributors as well as the manufacturer, whether based in the UAE or abroad (and not just to the entity that had direct contact with the consumer).

Although strict liability applies in product defect matters, proving causation may be challenging where an incorrect algorithm (as in the autonomous vehicle example above) gives rise to the harm, particularly in circumstances where the algorithm is embedded in a black box system that is not explainable (see below), and even more so where the algorithm is developed further by the machine learning process. Further, as discussed in our previous article titled '[Connected Cars, Autonomous Vehicle and Legal Potholes](#)',

delineating responsibility between the various parties involved in the development of AI products and services can be difficult, especially where the damage arises due to a malfunction or failure in more than one component simultaneously. In this regard, Article 291 of the UAE Civil Code currently provides *'If a number of persons are responsible for a harmful act, each of them shall be liable in proportion to his share in it, and the judge may make an order against them in equal shares or by way of joint or several liability'*. In practice, apportioning liability between a number of actors where such complex systems are involved, may prove to be rather challenging. On the other hand, the EU White Paper proposes that, in cases of 'significant harm', strict liability should apply to the person who: (a) benefits most economically from the AI system; and (b) has the most control over the risk associated with it. Again, determining who benefits most economically and who has the most control, is unlikely to be a simple exercise.

Privacy, discrimination and biased data

Although a small number of jurisdictions have enacted specific legislation (such as the Algorithmic Accountability Act in the US) mandating large technology companies to monitor and assess the accuracy, bias, privacy, accountability and cybersecurity of their AI products, the international trend has been for regulators and other organisations (including the UAE's Ministry of AI and Smart Dubai) to take a soft approach to regulation, mostly in the form of non-binding guidelines that are intended to foster development and uptake of AI in an ethical, transparent and responsible manner whilst minimising pitfalls such as discrimination and algorithmic bias. Although discrimination currently occurs even without the use of AI, the concern with algorithmic bias is that it would ingrain human bias and discrimination in 'black box' systems which are not able to detect in themselves such bias (let alone fix it), and as a result, risk perpetuating discrimination and inequality, particularly in the absence of human oversight.

Note that the UAE Federal Law Combating Discrimination and Hatred would also indirectly apply to AI systems (including AI powered recruitment systems) that provide outcomes which discriminate against an individual on specified grounds. In the absence of a legal regime where AI systems are granted separate legal personality and responsibility, it is the developers, distributors and utilisers of AI systems who remain liable for any breach of laws or losses arising from the use of such systems. For example, if a company were to deploy an AI staff recruiting system whose algorithm or data sets are discriminatory against women (because the data sets were from past job applications where the human assessors rejected candidates based on their gender), the company would be liable for the discrimination exhibited by the AI application.

Additionally, Article 38(1) of the proposed new DIFC Data Protection Law (which is undergoing consultation and yet to be enacted) provides *'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 significantly affects him or her'*. Examples of such an automated decision may include online credit applications or online recruitment tools, where there is no element of human intervention.

How to mitigate legal risks associated with the deployment of Artificial Intelligence

Accordingly, companies looking to deploy AI tools and applications need to:

1. obtain contractual warranties from the vendor that the AI system complies with all applicable laws and ethical use of AI guidelines. Even though guidelines may not currently be binding as law, they may form the basis of any future laws;
2. ensure legal requirements and ethics are embedded in the AI tools and systems 'by design'. For

- example, by ensuring that the AI algorithm is understandable and its decisions are explainable (reasons can be provided for a given input), noting that 'deep learning' systems may not be explainable, even to their developers;
3. employ diverse teams (in terms of age, gender, skill etc.) to help guard against the production of biased data sets;
 4. ensure the data set used is unbiased and reflective of the population, that it is not unfair to use the data even if the data is so reflective, and that the data is only used for ethical ends; and
 5. for companies established in the DIFC, provide a right to data subjects to object to decisions based solely on automated processing (including profiling) which significantly affects him or her.

For further information, please contact [Haroun Khwaja](mailto:h.khwaja@tamimi.com) (h.khwaja@tamimi.com).