Large Action Models - New types of risk?

Lidia Kamleh and Rajesh Vyakarnam of the Dubai Future Foundation talk about how to stay ahead of the curve with LAMs and mitigate the risks that may come with its use, while continuing to foster innovation and the adoption of AI within organisations.

AI was first widely introduced to the public through tools like ChatGPT. It was always expected to evolve and grow quickly and, within a year it had become the fastest-growing consumer software application in history, with over 100 million users.[1]

Today, we are on the cusp of "Industry 5.0", where the blending of science, humans, advanced technology, and machines will enhance human capabilities, focusing on personalisation, human-centric solutions, and sustainable development.

Developers and users continue to work fast comprehend the opportunities and challenges posed by the proliferation of the use of tools powered by large language models (LLMs). Countries around the world have established AI task forces, appointed AI tzars, published ethical guidelines and are working on AI-focused regulations.

LARGE ACTION MODELS

The latest evolution of AI, which has just found its way into consumer consciousness with products like Rabbit AI and Apple Intelligence features announced at Apple's WWDC2024, are large action models (LAMs).

LAMs are essentially AI models that have been built to understand complex user goals expressed in natural language. However, in contrast to LLMs or traditional AI, LAMs can translate the user's intentions into actionable steps in real-time, and execute them.

By connecting with external systems like IoT devices, LAMs are able to execute physical actions and retrieve or manipulate data. They can book appointments, make reservations, or complete forms by interacting with applications or systems as if they were a human user. Eventually, the technology could be deployed as a virtual personal

assistant (which is what Rabbit AI is being marketed as), full end-to-end process automation for customer service, processing customer returns from initial contact to actioning refunds, or even configured to execute procurement tasks on behalf of a company – restocking inventory when it runs low or purchasing replacements when an existing item is about to expire.

In a slightly eerie twist, LAMs could interact with additional layers of LAMs, and third parties may not know that they are responding to or collaborating with a LAM-powered solution.

Where traditional AI could be likened to a 2-dimensional rendering, in which AI systems are designed to perform specific, narrow tasks within well-defined boundaries, like a flat surface without scope or depth, LLMs extend the complexity by introducing an additional axis to create a 3-dimensional perspective. LLMs not only process language but also generate contextually rich responses and accept a greater range of inputs, like navigating a space with depth and volume, allowing for more nuanced and human-like interactions. As a further evolutionary step, LAMs could be compared to the metaverse, an expansive, interconnected virtual reality. LAMs transcend previous limitations, expanding on the ability to understand natural language prompts and generating content to enable autonomous decision-making, the execution of tasks via connected systems and learning, creating a dynamic, immersive environment that mimics the detail and interactivity of a fully rendered digital universe.

MITIGATING AI RISK

With greater opportunity and autonomy comes greater risk and technology has inevitably moved faster than the law. The release of AI-powered consumer software reinvigorated the discourse between regulators, consumer groups, insurers, lawyers, and the public.

When commercial and consumer contracts were first tested against what would now be called 'traditional' AI technology, they had to account for risks associated with AI models that are designed to process data to detect patterns, generate insights, automate processes and make predictions.

Risks flowing from issues like data protection, data leakage, intellectual property complexities, confidentiality, liability, insurance, bias and open-source licence compliance have been examined in courts around the world.

Generative AI has added a new layer of complexity to risk mitigation. The proliferation of these tools, which can synthesise new content, raises additional concerns over intellectual property infringement, erosion of user rights, and reduced human oversight. In the UK, the ICO recently issued a preliminary enforcement notice against Snap Inc and its UK subsidiary for alleged data protection failings in relation to its generative chatbot 'My AI'[2], which highlights the regulator's intent to present a clear message on intolerance for perceived failures to properly consider data protection when developing and implementing AI systems[3].

The convenience of generating satisfactory content and moving on to the next task has led users to place even greater trust in these increasingly autonomous models. The Getty Images v Stability AI case is ongoing[4], and will hopefully provide some guidance on the subsistence of intellectual property rights, and how AI models can be trained on publicly available, but protected, data.

With the advent of AI regulations such as GDPR and the forthcoming AI Act, user terms and conditions are evolving, presenting risks for both participants and non-participants. Consent forms are changing to reflect new realities. Key emerging issues include how AI agents operate on behalf of users and the legal implications of their actions.

AUTONOMOUS SOFTWARE AGENTS...

Given their ability to execute actions, with limited human input, and with the ability to adapt actions to meet perceived user needs, LAMs could be considered a form of 'agent', acting on behalf of the end-user. When LAMs act as an agent, it raises questions about the extent of the principal's (user's) liability for the agent's (AI's) actions. By contrast, even generative AI solutions cannot execute third party applications or interact with IoT systems in the same way.

Personal assistants, commercial agents and customer service agents are all bound by contracts and laws, which assign risk and responsibilities, nominate the applicable laws and expressly or implicitly set the repercussions for breach. Actuaries have

> "The imminent deployment of LAMs means that we are likely to see a blurring of jurisdictional boundaries, changing liabilities, and increased numbers of cross-border disputes."

calculated the costs of those risks, and the price to mitigate them.

LAMs, therefore, further extend the possible heads of liability. As LAM-enabled AI systems learn over time and execute actions which vary and adapt to the perceived user goals, those actions may trigger liability under consumer protection laws. There are very few consumer protection laws (with the notable exception of the Automated and Electric Vehicles Act 2018, UK (the "AEV Act")) that define statutory liability for damage caused by autonomous systems.

Another example of a head of liability, in the workplace, is that LAMs could, without sufficient regulatory safeguards, unfairly amplify discriminatory treatment of individuals or groups, taking actions on behalf of an employer thereby triggering liability under employment or anti-discrimination laws.

Now, perhaps, owners or operators of LAM-enabled systems could be held liable as principles to their LAM agents – without the ability to hold their agents accountable or obtain suitable insurance.

The AEV Act has set a statutory benchmark by attributing liability for loss to the insurance underwriter, when damage is caused by a vehicle in autonomous-driving mode. However, the scale, complexity and potential severity of the risks involved with deploying autonomous LAM agents, with the possibility that they may interact with each other with no (or minimal) human safeguards, means that insurance underwriters are likely to struggle to fully assess risk, impose significant policy exclusions and proportionately assess premium costs. The AEV Act could, therefore, be too limited in use-case context and may not be a useful point of reference in other sectors where LAM-enabled solutions are deployed.

The imminent deployment of LAMs means that we are likely to see a blurring of jurisdictional boundaries, changing liabilities, and increased numbers of cross-border disputes.

The 'Navigating Megatrends Shaping Our Future in 2024'[5] report from Dubai Future Foundation highlighted the need to regulate specific AI use cases rather than the technology itself. Contracts will therefore have to drill even further into the deployment scenarios for each LAM solution, and regulate the limits of its agency, specify its autonomy, prescribe the systems it can connect to and actions it can execute. As a first step, multinational organisations like EU, OECD and UNESCO have all published guiding principles and ethical recommendations for the development and adoption of AI technologies. More substantive regulations and national laws are in progress globally, and thought will have to be given on how to roll out suitable changes to multilateral framework terms like the ICC's Incoterms or FIDIC's books.

Users might perceive the risks of LAMs as similar to a toddler inadvertently making in-app purchases on an iPad. However, like toddlers, LAMs will develop rapidly. During LAMs maturity cycle, the urgency to establish comprehensive, use-case-specific regulatory frameworks grows. The pace of technological evolution demands proactive and collaborative efforts to safeguard innovation while minimising risks.

To stay ahead of the curve with LAMs while fostering innovation, we need to craft smart regulations, promote cross-sector collaboration, and invest in transparency and security. Only those who innovate responsibly will thrive.

The Dubai Future Foundation is dedicated to driving innovation and shaping the future of the Emirate of Dubai. The team at DFF Legal is excited to engage with innovators in the legal sector to shape policy and regulation. You can find out more about our initiatives and how to be part of the discussion at https://www.dubaifuture.ae/

References 1 - 5 are available on the web version of the article on the Oath's website.

Text by:
1. LIDIA KAMLEH, *chief of legal affairs, Dubai Future Foundation*
2. RAJESH VYAKARNAM, *senior counsel, technology, Dubai Future Foundation*