

Science Update

Artificial intelligence: uses, risks and “trustworthiness”

Introduction

In its April 2018 Communication on “*Artificial Intelligence in Europe*”, the European Commission defined AI as:

“systems that display intelligent behaviour by analysing their environment and taking actions – with some degree of autonomy – to achieve specific goals.”¹

The simplicity of this statement belies the breadth of different technologies encompassed within it. Researchers have proposed multiple more granular ways to classify AI systems: some based on the **nature of the action** carried out (for example, “*speech to text*”, or “*image recognition*” technology); others on the basis of the underlying technology (“*speech to text*” is a subset of “*natural language processing*” technology) and still others dependent on the **level of advancement of the technology** in question (“*deep learning*” is in fact a more technologically advanced subset of “*machine learning*”, which in turn is just one type of AI rather than synonymous with the term).

As evident in the breadth of these categorisations, AI systems operate in many different ways, and in fact there are many different forms of AI currently in development. These include systems which “learn” by a reward/punishment system, learn by copying examples provided, learn by analysing data provided using mathematical principles or a neural net where multiple inputs result in reinforcement of the most advantageous results.

Uses of AI relevant to products

At present, different types of AI permeate all aspects of the consumer products sector, and AI-based systems are already active in everyday objects. Smart voice assistants on our mobile phones or speakers rely on natural language processing to convert speech to recognisable commands for the “assistant” to execute; meanwhile it’s an AI system parsing a vast database in seconds that enables your device to recognize the audio signature of music

played on your phone and display the name and artist on the screen.

In the healthcare sector AI systems such as IBM Watson are already being used to facilitate new drug target identifications. On a more general level relevant to both the consumer and healthcare spheres, AI systems are poised to be crucial in the effective deployment, continuous monitoring and operation of the 5G networks that promise to power the future of IOT products.

AI also has a particular role to play in product design and monitoring product safety. Through integration within the manufacturing phase (particularly testing and development) AI has the potential to facilitate the production of safer, more effective and more sustainable products. And, the potential of AI systems to scan the internet for early indicators of issues reported with products which indicate a need for corrective action or recall, may herald a significant change in the field of product safety.

Risks of AI relevant to products

The potential risks are wide ranging. Aside from the significant issues of breaches of privacy and lapses in cybersecurity which represent serious risks particularly where reliance on a data-driven system is concerned (and which we discussed extensively in relation to the GDPR in our last issue),² there are very real risks associated with the potential opaqueness of the computations involved in any AI-system, including problems with the system’s ability to acquire and process data.

Particularly with systems that do not rely on existing data stores or active input from human sources to form the basis of their operations, but instead are advanced enough to collect their own data (think of a self-driving vehicle continually gathering information about road and traffic conditions) and perform automated data extraction, there are multiple scenarios where things may go “wrong”, and lead to some level of injury to humans. For example, the camera sensor on a robot or vehicle may not be able to operate in low light, or point in

¹ Communication Artificial Intelligence for Europe (April 2018) <https://ec.europa.eu/digital-single-market/en/news/communication-artificial-intelligence-europe>.

² See Valerie Kenyon and Anthea Davies, “Data Protection and “smart” products: a new perspective on safety”, *International Products Law Review*, Issue 74, p. 12

the wrong direction, such that despite sophisticated programming to facilitate navigation around difficult terrain the robot “falls at the first hurdle”.

As a more complex problem, the nature of machine learning is such that actions are considered on the basis of the probability that each action is the right one rather than on the basis of strict instructions. As such it is possible that an algorithm could select an outcome unforeseen by the creator of the device – which could have catastrophic consequences, including physical harm to persons. As AI grows more sophisticated, it may become increasingly difficult to “unpick” the process and identify the point at which a poor decision was made. This leads to an increasingly complex landscape for who should be attributed liability in these circumstances, and has led (as previously discussed in this publication)³ to the controversial suggestion of attributing legal personhood to the AI system in question.

The evolution of “Trustworthy AI”

Given the potential issues, is there a direction of growth for AI that prioritises risk-management and ethical development? EU policy-makers certainly think so. In June 2018 the European Commission set up a High-Level Expert Group on Artificial Intelligence (the “**Expert Group**”), comprised of a variety of stakeholders in AI across academia, civil society and industry. On 8 April 2019, the Expert Group published its first deliverable: *Ethics Guidelines for Trustworthy AI* (the “**Guidelines**”).

The Guidelines set out a particular vision of Europe’s goal for a human-centric AI, aiming for an ethical framework which would promote the development of what has been titled “Trustworthy AI”. Trustworthy AI consists of AI systems that are **lawful** (compliant with applicable laws and regulations), **ethical** (ensuring adherence to ethical principles and values, and **robust** (both from a technical and social perspective, particularly recognising that even with good intentions AI systems can cause unintentional harm).⁴ The three headline ethical principles outlined are respect for human autonomy,

prevention of harm, and fairness and explicability. Seven key requirements are then elucidated for ensuring these principles (for example human agency and oversight; technical robustness and safety; privacy and data governance).

The Guidelines also provide a checklist, or “assessment list” to be used by stakeholders in developing and utilising their AI systems. From 26 June 2019 to 1 December 2019 the assessment list is undergoing a piloting phase during which stakeholders are invited to test the list and provide practical feedback on how it can be improved.

Following this, on 26 June 2019 the Group published its second deliverable: *Policy and Investment Recommendations for Trustworthy AI* (the “**Recommendations**”). The 33 recommendations clearly signal the EU’s ambition to emerge as a competitive and sustainable force in the sphere of a very specific kind of AI revolution: one which empowers and benefits humans. Having identified four key sectors crucial to the development of AI (public; private; general society; and research and academia), the Recommendations then discuss four key enablers that may set the correct foundation for the proliferation of ethical AI: data and infrastructure; education and skills; governance and regulation; and funding and investment.

What about liability for Trustworthy AI?

The Guidelines do not engage in detail with the “lawfulness” aspect of Trustworthy AI. However they do remind us that some existing rules at European, national and international level may already apply or be relevant to the development, deployment and use of AI systems today, including existing civil liability and product liability regimes. This is a welcome reminder for stakeholders in the area to not assume their potentially novel product, or AI system, is automatically excluded from the scope of any existing general or sector-specific regimes. In fact, two of the questions included in the current draft of the assessment list are designed to prompt this awareness:

³ See Christelle Coslin and Gunou Choi, “Artificial Intelligence: what’s the plan for France?”, *International Products Law Review*, Issue 73, p.20

⁴ As summarised on page 4 of the Ethics Guidelines.

“Did you assess whether there is a probable chance that the AI system may cause damage or harm to users or third parties?”

“Did you consider the liability and consumer protection rules, and take them into account?”

The Recommendations do identify governance and regulation as a key foundational layer which will enable the development of AI and suggest a comprehensive mapping of existing EU laws to assess the extent to which the laws are still fit for purpose in an AI-driven world. At least in the context of product liability, this mapping exercise is already underway. As we have previously discussed in detail in this publication⁵, the question of whether the Product Liability Directive applies to various AI technologies has been under significant scrutiny in the past year and the publication of the European Commission’s guidance on this later in 2019 will be a welcome development in providing clarity in this area.

Until then, the Recommendations signal some clear policy positions which may indicate the direction of future discussions around liability for AI systems in Europe. In particular, recommendation 29.7 urges policy-makers to refrain from establishing legal personality for AI systems or robots. Meanwhile, recommendation 27.2 suggests traceability and reporting requirements to facilitate the auditability of AI, an obligation for meaningful human intervention when using AI in specific sectors (for example, human doctors checking medical treatment decisions), and supplementing civil liability frameworks with mandatory insurance provisions to ensure adequate compensation in case of harm.

Comment

We would recommend that all parties involved in the development, use, and utilisation of AI systems carefully monitor the progress of the Expert Group and the discussions its publications inspire within the European Commission, as well as keep a lookout for the European Commission’s forthcoming guidance on the Product Liability Directive.



Adeela Khan

Associate, London
T +44 20 7296 2862
adeela.khan@hoganlovells.com



Marion Palmer

Senior Scientist, London
T +44 20 7296 5110
marion.palmer@hoganlovells.com

⁵ See Matthew Felwick et al, “Under the microscope: is the European Product Liability Directive fit for the tech revolution?”, *International Products Law Review*, Issue 73, p.6