

Find more resources in the ACC Resource Library: www.acc.com/resource-library

Top Ten Issues on Liability and Regulation of Artificial Intelligence (AI) Systems

By Tarek Nakkach,
Region Legal Counsel, UKIMESA, Hewlett Packard Enterprise

August 2, 2021

Key Takeaways:

- *New Artificial Intelligence (AI) technology is being integrated into all industries.*
- *In-house counsel need to be aware of the gaps in regulation and law for these emerging technologies.*
- *In-house counsel need to be aware of the legal and ethical issues around the adoption of AI technology.*
- *Examine and research what type of insurance is available for your company with AI technology.*

I have written a few articles regarding the liability of autonomous systems under the United Arab Emirates' (UAE) law, [regarding the liability of autonomous systems under the UAE's Civil Code, available remedies, comparing to other regimes,](#) and [recommendations for law, policy and ethics.](#)

I focused mainly on the liability and regulation of autonomous or Artificial Intelligence (AI) systems under the laws of the UAE, but I also compared the UAE's legal system to other regimes, including the United Kingdom (UK) and the European Union (EU). I concluded that generally speaking, when it comes to AI, the issues are similar across the globe.

In the near future, every single one of us will be dealing in some shape or form with an autonomous system or an AI-powered system. We may have done so already in our daily lives as consumers, when we called our bank to inquire about a service and on the line was the bank's intelligent automated assistant, or when we used a website and the AI bot replied to our complaints. Soon we may be riding in autonomous vehicles, or undergoing surgery performed by a robot.

In our capacity as in-house counsel, and regardless of our industry sector, we will be dealing with AI. Whether our companies are installing the latest systems that will run analytics to drive better results, whether we work in technology and our company offers AI solutions to customers, we will deal with AI liability issues and will be asked to provide advice. I hope this article will shed some light on the most important regulatory and liability issues (in no particular order) when dealing with an autonomous system.

1. Human Control

The first question to assess when dealing with an AI system, is whether it is fully autonomous or semi-autonomous. In a semi-autonomous system, there is a significant level of human control, where a person can manage the system. For example, a medical diagnostic system which analyses a patient's medical history, assesses their condition, and provides advice on treatment. The doctor will then be able to take that advice and decide on a treatment. There is human control, and liability ultimately is with the medical practitioner.

What if instead of a doctor, the system directly provides a diagnosis and treatment advice to the patient? The system is then fully autonomous. If such a system makes the wrong diagnosis and the patient is injured or worse, dies, who is liable? The designer of the system, the supervising doctor, or the hospital?

Let us take another example, in a corporate setting. There are many AI-powered legal solutions that have been marketed for in-house counsel recently. The most prominent ones are automated contract negotiation solutions, where the "smart" system identifies for example the riskiest clauses and suggests alternative wording. In this scenario, the system is not fully autonomous, as it is merely suggesting a pre-populated standard wording, and it is up for the in-house counsel to accept or reject the suggestion. Therefore, the responsibility for the contract draft ultimately lies with the lawyer. Can we imagine a scenario of full autonomy when the technology evolves, where the system not only "suggests" but actually performs changes to a contract? Can we also imagine a scenario where both parties are negotiating a contract without human intervention? When this type of technology becomes a reality, how would we as in-house counsel react - will we embrace it or resist?

2. Liability for Harm or Damage

The main existing liability framework applicable to AI systems causing harm to a person is tort liability. While tort liability gives rise to compensation, there are also strict liability and product liability regimes, in instances where the product, a car for example, causes harm due to a manufacturing defect.

In all cases, the liability regimes are wide enough to offer an injured person redress. However, in the case of fully autonomous systems, there is a gap in the current legal systems. When the system is fully autonomous i.e., it is learning from "experiences" while in its implementation phase and is therefore able to take a decision without human control, then most of the current legal regimes are unable to provide adequate protection for injured persons.

In simple terms, a manufacturer can be held liable for production defects, a hardware malfunction, a software bug. However, when the AI system has been deployed without defect, learns from its surroundings (such as in the case of autonomous cars), or from large amounts of data (such as in the medical example mentioned above) or from the

internet, and causes harm, then there may be a [gap in responsibility under the current legal frameworks](#).

3. Liability for Data Privacy Breaches

When speaking of harm, we tend to think of bodily harm. The examples above regarding medical diagnosis, or an autonomous vehicle running over a person, come to mind. What about harm caused by a breach of privacy rights? What if an AI system somehow leaks personal information, or posts it on Facebook. Who is then liable?

Most AI, or more particularly search algorithms, [use machine learning](#) to run analysis and provide us with tailored ads. The more the technology evolves, the more it is able to intrude on our privacy rights. Take face recognition technology as an example, there were concerned voices, especially in the US, regarding risks of falsely identifying suspects in criminal cases. This is why in the United States, some states introduced bills to ban certain uses of this technology. This is a classic example of where liability and regulatory issues coincide regarding AI.

4. Insurance

Insurance is one of the solutions contemplated - in the United Kingdom for example - to cover any legislative gap, with the introduction of [Automated and Electric Vehicles Act 2018](#). As a reminder, the gap identified regarding fully autonomous systems stems from the fact they continuously learn from their environment, and that “defects” may no longer be attributed to the manufacturer of the system. This regulation is an ad hoc solution for autonomous vehicles but does not cover all types of autonomous systems.

Therefore, one of the first adjustments that can be made is to make sure an injured party receives compensation for the damages he or she suffered, through insurance. This avoids the need — at least for now — to go into detailed debates about which party is liable in case of injury and wait for the courts to decide on matters or for authorities to issue complex regulation

As in-house counsel, when negotiating a contract with an AI service provider, we may require that they have AI or Machine Learning insurance, to make sure the liability gap is covered.

5. Accountability

In order to determine liability, there should be accountability. The main problem with fully autonomous systems such as those [running on complex neural networks](#) is to determine why and how AI makes the decisions it does. Think of it like the human brain function: thoughts and decisions. The actions can be seen but can someone be 100% sure how the decision has been made? Unlikely. This is why in AI, such a system is considered somewhat of a black box, and it is up to the designers of the system to be able to explain how a certain decision has been made so there will be responsibility and

accountability. This is where regulation may be key, to ensure accountability when an AI system is deployed.

6. Safety

Safety is key and the most important point around AI. We need to ensure that AI systems are deployed safely. This is a major question in transportation and healthcare. At the [Assuring Autonomy International Programme at the University of York](#) where I am a fellow, we specialize in research regarding the safety of autonomous systems. This is what regulators are most worried about. The UK has recently issued a [consultancy paper on Automated Lane Keeping Systems](#) as a suggested regulation for self-driving cars. I expect more guidance to follow as the technology becomes readily available.

7. Soft Law vs Regulation

The concept of tech neutrality was introduced some time ago as a generally acceptable regulatory approach. As explained by FCAI, the [concept means that](#) *“legislation is drafted in a manner that is not bound to any specific technological form or method. The objective is two-fold. First, to enable legislation that lasts the test of time and does not become outdated when technology develops. Second, to treat different technological solutions equally and without inadvertently granting unfair advantage to certain solutions while discriminating others.”* ([“Regulating AI – Is the current legislation capable of dealing with AI”](#), FCAI, October 20, 2020)

While there is resistance to regulating technology, soft law may be a way forward, at least for the time being- for AI. What does soft law mean? In the AI context, it is simply issuing a set of principles that will govern the use and deployment of AI.

The EU has decided however to take a different approach, with its [Proposal for a Regulation laying down harmonised rules on artificial intelligence \(the Artificial Intelligence Act\)](#).

This may be the most important piece of regulation that will be introduced on AI. The objectives of the regulation are the following:

- ensure that AI systems placed on the Union market and used are safe and respect existing law on fundamental rights and Union values;
- ensure legal certainty to facilitate investment and innovation in AI;
- enhance governance and effective enforcement of existing law on fundamental rights and safety requirements applicable to AI systems;
- facilitate the development of a single market for lawful, safe and trustworthy AI applications and prevent market fragmentation.

The EU has adopted a risk-based approach, where certain high-risk applications are bound to strict requirements - as opposed to “low risk” AI applications, which are subject to less stringent requirements. An AI powered contract management system would most

likely fall under low risk, whereas a self-driving car system would be subject to stricter requirements.

8. AI Ethics

AI systems are basically the products of their designers. As a result, many ethical issues found in society when it comes to human interaction can be replicated in the field of AI. Issues include AI bias, privacy, transparency and accountability. Many of the big players have developed principles to guide their own work in AI, including [Microsoft's "Responsible AI"](#) and others.

Hewlett Packard Enterprise is also working on [AI Ethics and Principles](#). One of the key issues of AI Ethics is AI bias. According to the HPE AI Ethics and Principles, AI should be:

1. **Privacy-enabled and secure** – respect individual privacy and be secure.
2. **Human focused** – respect human rights and be designed with mechanisms and safeguards, e.g. to support human oversight and prevent misuse.
3. **Inclusive** – minimize harmful bias and support equal treatment.
4. **Responsible** – be designed for responsible and accountable use, inform an understanding of the AI, and enable outcomes to be challenged.
5. **Robust** – be engineered to build in quality-testing and include safeguards to maintain functionality, and minimize misuse and the impact of failure

9. AI Bias

Bias is one of the main issues when dealing with algorithms. This is a complex subject, as discrimination is not strictly speaking a “privacy” issue but more of a social issue. [AI bias is in a way like human bias where a person makes a wrong assumption, based on race or gender](#). Similarly, a system that is fed with “prejudiced” data or corrupt data, would reach wrongful/discriminatory results. There are many examples of AI bias.

This is why in the United States, the [Wyden-Booker bill](#) was introduced to the US Senate to tackle this issue using the wording “automated decisions” While the bill was not successful, it may be reintroduced under the Biden administration.

How do we avoid AI Bias? While regulation is key, developers have a duty to carefully collect and process data that might have an effect on AI bias. In-house counsel working with such developers should ensure that the data collected is from different genders, ethnicity, cultures, etc. to avoid bias.

10. Intellectual Property

AI will create songs, novels, and even pieces of art, which begs the question: Who owns the copyright of such creation? Can AI creations be patented? The same questions that we encountered regarding liability and ethics are valid for Intellectual Property (IP). Do we need to change any of our existing IP policies? The [World Intellectual Property](#)

Organisation (WIPO) thinks so. For in-house counsel working in IP or regularly filing patents for innovative technologies, the WIPO guidelines give a good perspective of what's to come.

While it seems AI is raising more questions than answers at the moment, it is generating a lot of debate amongst regulators and technology companies. For anyone still doubting that AI is the future, just check the National Artificial Intelligence Initiative of the US Government at <https://www.ai.gov/> to have an idea about what to expect.

I believe AI is extremely exciting - we get to discover the technology as it evolves, and the legal community's response. I can't wait for what the future holds!

Author: Tarek Nakkach, Region Legal Counsel, UKIMESA, Hewlett Packard Enterprise

Check Out Additional ACC Resources:

- [IT, Privacy, and eCommerce Network](#)
- [“Artificial Intelligence and Regulatory Compliance”](#), by Emily Foges, Emma Walton, ACC Docket, January 2, 2020
- Search the [ACC Resource Library](#)
- Not a member? [Join ACC Today!](#)

Disclaimer: The information in this resource (or in any resource collected in ACC's virtual library) should not be construed as legal advice or as a legal opinion on specific facts, and should not be considered as representing the views of its authors, its sponsors, and/or ACC. These resources are not intended as a definitive statement on the subject addressed. Rather, they are intended to serve as a tool providing practical guidance and references for the busy in-house practitioner and other readers. For legal advice or representation, please engage a legal counsel.

© Association of Corporate Counsel. All rights reserved. Visit www.acc.com