Artificial Intelligence and contracts: shaping standards

December 20, 2018

With this article, we will address some legal issues arising from contracts featuring AI-based services/products.

So far, commentators on contracts and AI have mainly focused on the data protection and cybersecurity aspects (including, for instance, security measures, privacy-by-design / default, review of decisions based on automatic processing, data portability, etc.)

With this post, we will address some additional aspects to be taken into account when considering AI-based contractual arrangements:

- **Applicable law**. A first element is the choice of the applicable law. Any party generally prefers to apply the laws of its own jurisdiction to any agreement it enters into, in order to avoid unknown implied terms. When dealing with AI, this has become an even more crucial element, considering that currently EU (and member states') laws do not provide for a specific legal framework for AI (and robotics), with wider room for—unknown and implied—terms t creep into the contract.

  Just consider, for example, a contractual arrangement for the supply of a robot employed in industry manufacturing and related services. Under Italian law, such arrangement may involve the (cumulative?) application of the Italian civil code provisions related to the following types of contracts:

  A. Sale and purchase *(vendita)*

  B. Lease agreement *(locazione)*, for the license of IPRs

  C. Service agreement *(appalto di servizi or prestazione d'opera,* depending on the nature of the relevant obligations)

  According to the Italian Civil Code, provisions dealing with each of the above contracts imply different approaches on many important topics, including (a) warranties/fitness for a particular purpose; (b) liability; and (c) passing of risk to the purchaser.

  In light of the above, we recommend carefully choosing a familiar applicable law, also taking utmost care in defining contractual scope of activities, i.e. the actual obligations borne by the parties.

- **Insurance and SLAs**. AI liability is a widely debated topic (see here). Under "traditional" outsourcing contractual arrangements, SLAs (and the related obligation to pay a penalty) are generally devised to avoid 'low grade' issues that might arise, for instance, if processes are not followed properly. This applies to human beings who are by definition fallible and more or less efficient depending upon a large number of factors. AI based services are mainly performed through automatic means (meaning human intervention is very limited) with a lower degree of unreliability. However, AI failures, when occurring, are more likely to be catastrophic (e.g. total service outages.)

The parties to an AI based contract will accordingly have to be more creative in setting up procedures that grant continuity of the services / product defects, setting up additional safeguards to address "catastrophic failures" (which are *per se* also "material breaches" of contract.)

A higher liability cap may be considered, further detailing the parties' share of liability that should effectively take into account each party's role, including the so-called "wrong data feeding."

Within this scenario, an adequate insurance coverage becomes fundamental (with the related insurance costs to be likely factored in the provider's service fees.)

- **Intellectual Property rights**. "Traditional" IT service agreements dealing with the creation or transfer of IPRs generally contain a clause whereby the parties: (i) maintain their respective IPRs pre-existing to the effective date of the agreement (so called "IP background rights"); and (ii) regulate the ownership of the IPRs arising from the performance of the agreement.

  There are a number of open-ended questions. What criteria should be used to define "own intellectual creation" for works arising from the activity of computers and robots equipped with AI? Will the request of the EU Commission—to support a "horizontal and technology-neutral approach" to "robotics IPRs"—to EU Parliament be followed-up?

  A clear regulation of the ownership of the IPRs arising from trained AI is crucial. Indeed, most of such IPRs may be created through automatic means, i.e. by "subjects" (robots/systems) which may not be considered as "authors" within the meaning of EU copyright and patent law (see here).

- **Audit rights and black box**. Customers' audit rights should be shaped differently. Traditional IT sourcing models generally provide for auditing work / services carried out / managed by humans, mainly through the review of documents, reports and procedures. A human being can check the work of another human being. It may well be harder to assess how an AI system actually works, clearly identifying the AI "decisions" patterns, criteria and underlying logic.

  Within this scenario, the implementation of a black-box system would enhance the effectiveness of customers' audit rights, as: (i) the audit activity would be "continuous," rather than based on the planned audit schedule; and (ii) the information collected by a black box would be more comprehensive and analytical.

  By way of example, we are observing a number of companies involved in the provision of IT tools to carry out remotely audits related to health and safety in the workplaces (e.g., the head of security carries out audits, in real time, through visors/sensors located in other jurisdictions, etc.)

- **Competition**. In 2015, the EU Commission launched a public consultation on *"data-driven industries."* Among others, the EU Commission focused its attention on antitrust issues related to the ownership of huge (big)data sets by incumbent OTT operators.

  The EU Commission argued that, under certain conditions, a data set might be regarded as an "essential facility," so that owners of such "essential facility" (like an internet backbone, a railway, a non-replicable utility network) might be compelled to (a) enter into contracts with each requesting stakeholder; and (b) apply fair, transparent and non-discriminatory conditions to their counterparties.

  Should this approach be confirmed by EU law provisions, we may face a disruptive change of contractual arrangements concerning big OTT operators and internet publishers.

- **Dual-use.** “Cyberwar” is one of the most “feared” threats of the 21st century. Such a “fear” is based on a fact: most AI products/services may be used for both civil and military purposes. Dual-use regulation is particularly complex within the EU, and there are several different regulatory approaches worldwide. The contract should take into account adequately all dual-use implications.

- **Knowledge transfer**. In AI-based contractual arrangements, we will face no – or minor – transfer of knowledge from AI provider to customer. This may lead to new types of “vendor lock-in,” i.e. an increasing economic dependency of the customers vis-à-vis service providers. Exit provisions will have to address how to reimport information, where appropriate also regulating data ownership (e.g. own the IPR in the data generated through the education provided by the customer to the robot). Ad hoc representations and warranties will have to be further required to address knowledge (and data) management.

New contractual standard for AI-based arrangements are being shaped. From an Italian law perspective, this will lead to contracts being more specific, particularly where conflicting civil code provisions may apply.

We welcome any question you may have on this topic. Contact our Dentons Italy TMT Team at tmtbites.italy@dentons.com and do not forget to sign up to our TMT Bites Newsletter!

Your Key Contacts

Giangiacomo Olivi
Partner, Milan
D +39 02 726 268 00
M +39 344 27 62 550
giangiacomo.olivi@dentons.com