WORKSHOP

LIABILITY IN THE AREA OF AUTONOMOUS SYSTEMS AND ADVANCED ROBOTS / IOT-SYSTEMS

13 JULY 2017, 10.00-16.30
BERLAYMONT, RUE DE LA LOI 200, 1049 BRUXELLES (ROOM WALTER HALLSTEIN)

Aim of the workshop

The objective of the workshop is to discuss questions regarding liability in the area of autonomous systems and advanced robots / IoT-Systems. The workshop will mainly explore the specificities of autonomous systems and advanced robots / IoT-Systems compared to "traditional" machinery and discuss these specificities in relation to liability schemes. As in the business-to-business area questions of liability currently seem to be addressed by contracts, the workshop will focus on damages incurred by natural persons.

Background

On 10 January 2017, the European Commission adopted the ''Building a European Data Economy'' Communication, accompanied by a Staff Working Document. In parallel, a public consultation on data economy was launched and a structured dialogue with stakeholders was announced. This workshop is part of this dialogue. It explores possible avenues for addressing any shortcomings and the start of a wide structured dialogue with stakeholders and Member States on these topics. A preliminary analysis of the contributions to the consultation can be found here.

In parallel, the Commission also conducted a public consultation on the evaluation of the Product Liability Directive (85/374/EEC). This exercise also seeks to assess the adequacy of existing liability rules when damages arise in the context of autonomous systems and advanced robots/IoT-systems. A brief factual summary on the results of the consultation can be found here.

Autonomous systems and advanced robots may act in a way which was not foreseeable at the time when the system was produced or put into operation. Such autonomous actions may cause harm to humans or damage to other objects. As a consequence of the technological progress the complexity of algorithms governing autonomous systems and advanced robots increases, resulting in systems with sophisticated self-learning capabilities and increased autonomy. Increased autonomy may potentially increase productivity, prevent human failures and improve safety. Even if a human still makes the decision artificial intelligence can still be very beneficial in helping them reach this decision, e.g. predictive maintenance, providing data which you can use to optimize the production process, reducing electricity costs etc. Nevertheless, the more autonomous a system gets, the more difficult it can be to foresee its future decisions and actions when creating/developing it.

In addition to the autonomy, also the different layers of components that compose IoT systems increase the complexity of liability issues. The combination of connected objects that can communicate with each other as well as with humans makes it difficult to assess the contribution of each component to an act or decision of the system as a whole. The level of complexity further increases when the system is not provided as such by one single producer but is rather composed of hard- and software components from different providers.

Given the peculiarities of systems equipped with artificial intelligence, the multi-layer structure in the IoT environment and the connection to the internet, it is worthwhile to assess the adequacy of traditional liability rules on these systems with regard to damages incurred by natural persons.

It is also getting increasingly difficult to differentiate a product from a service. While IoT systems have a physical embodiment (and could thus be considered a product), their main added value is derived from them being embedded in a network and the service that is provided through this network. It is not entirely clear whether such hybrids are covered by the current liability framework.

Topics for discussion

First Cluster

The first cluster of this workshop will deal with the technical characteristics of autonomous systems and advanced robots / IoT Systems which are equipped with artificial intelligence. The difference between "traditional" machinery and systems which are operated by applying complex algorithms and capable of self-learning shall be further examined. .

The Product Liability Directive (PLD) deems a product to be defective if it does not provide the safety which a person is entitled to expect, taking all circumstances into account. It has to be clarified whether unintended, autonomous behaviour would be covered by this definition. With learning systems, it is not entirely clear whether the producer can always be held liable.

Liability under the PLD is excluded if the producer proves that, having regard to the circumstances, it is probable that the defect which caused the damage did not exist when the product was put into circulation. Moreover, most of the Member States allow for a "Development Risk Defense" set out in the PLD. The "Development Risk Defense" allows producers to defend themselves by proving that the state of scientific and technical knowledge at the time when the product was put into circulation was not such as to enable the existence of the defect to be discovered. Therefore, it is useful to discuss whether there is a gap in the current EU and national liability regimes which could inhibit injured persons from recovering damages when an autonomous systems or advanced robot / IoT-System harms them or damages an object while this could not have been foreseen at the time the system was created.

On the European level, there is a series of EU safety legislation, e.g. the Machinery Directive that deals for example with industrial robots, under which economic operators (manufacturers,

importers, distributors) are responsible for the safety of the products, placed on the EU market, that must guarantee the health and safety of persons when the product is used as foreseen or reasonably foreseen.

In addition to the evolutionary changes of an autonomous system due to its self-learning capabilities, the operations of autonomous systems and advanced robots / IoT systems may also be influenced by human intervention. This cluster will examine how the operations of autonomous systems and advanced robots / IoT Systems are supervised in practice, be it by the system itself or by humans. Despite the autonomy of autonomous systems and advanced robots / IoT-systems, supervision by humans might still be necessary. The possible needs for supervision as well as the existing opportunities for human supervisors to interfere are factors which could play a role in the allocation of liability. However, a possible requirement of supervision would conflict with the autonomy of an autonomous systems and advanced robots / IoT system as the idea of an autonomous system is to increase productivity by shifting (parts of) the decision making process to the system. This cluster should examine the balance between the benefit of autonomy and a possible need for supervision.

Second Cluster

The second cluster will analyse to which extent the complexity of autonomous systems and advanced robots / IoT Systems impacts on the detection of defects. Whereas the occurrence of damage can usually be proven without undertaking major efforts, retracing the way from such damage to a defect may prove to be more difficult. The level of complexity increases with the number of layers which constitute the Robots / IoT System as well as with the intricacy of the algorithms that ensure the system's autonomy. In this respect, whether all Robots / IoT Systems will need to be equipped with event data recorders that save log-data, which log-data are saved and by whom such log-data is accessible needs to be analysed. In addition to access to the log-data, you also need the ability to draw conclusions from such data in order to evaluate what happened and possibly detect the origin of a defect. This can depend on the way log-data is presented, its interoperability and the existence of experts who could evaluate log-data for individual victims or other parties involved such as insurance companies.

Third Cluster

Liability issues linked to defects arising from unwanted interference from outside such as cyberattacks are the subject of the third cluster. The protection against cyberattacks will need to be adapted and improved over the lifetime of autonomous systems and advanced robots / IoT Systems. This cluster will examine how these adaptations and improvements could be achieved and which party should be responsible for an up-to-date protection of the system.

To attend, please register **here** by **07 July 2017**.