NEW CHALLENGES IN THE EUROPEAN COMMISSION'S "REPORT ON THE SAFETY AND LIABILITY IMPLICATIONS OF ARTIFICIAL INTELLIGENCE, THE INTERNET OF THINGS AND ROBOTICS"

SERGIO GUIDA

Independent Researcher, Sr.Data/Information Governance Mgr.

Key-words: Artificial Intelligence - Internet of Things - robotics - liability - safety

Category: Legal Area

On 19 February 2020, the Commission has published for stakeholders' consultation its AI White Paper whose overall goal is, based on European values, to promote the development and deployment of AI (Artificial Intelligence), by adopting new specific legislation to address the risks of AI and other new emerging digital technologies. A report on the safety and liability implications of AI, the Internet of Things (IoT) and robotics was published alongside the White Paper, recognising the importance and potential of these technologies and the commitment to making Europe a world-leader in them.

The overall objective of the safety and liability legal frameworks is to ensure that all products and services, including those integrating emerging digital technologies, operate safely, reliably and consistently and that damage having occurred is remedied efficiently.

Along with the opportunities that AI, IoT and robotics can bring to the economy and our societies, they can also create a risk of harm to legally protected interests, both material and immaterial ones, so they should integrate safety and security-by-design mechanisms to ensure that they are verifiably safe at every step, taking at heart the physical and mental safety of all concerned.

The challenges brought by the digital emerging technologies can be summarized as follows.

- Connectivity is a core feature in an ever-growing number of products and services. This feature is challenging the traditional concept of safety, as connectivity may directly compromise the safety of the product and indirectly when it can be hacked leading to security threats and affecting the safety of users. Industrial applications may also be exposed to cyber threats affecting the safety of persons at larger scale when such applications lack the necessary levels of security. This can be the case for example of cyber-attacks on a critical control system of an industrial plant.

Union product safety legislation does not generally provide for specific mandatory essential requirements against cyber-threats affecting the safety of users. However, there are provisions related to security aspects in the Regulation on Medical Devices, the Directive on measuring instruments, the Radio Equipment Directive, or the vehicle-type approval legislation. The Cybersecurity Act sets up voluntary certification framework for Information and communications technology (ICT) products, services and processes while the relevant Union product safety legislation sets up mandatory requirements.

- Autonomy is one of the main features and AI based unintended outcomes could cause harm to the users and exposed persons. Although the Union safety framework already sets obligations for producers to take into account in the risk assessment the “use” of the products throughout their lifetime, the self-learning feature of the AI products and systems may enable the machine to take decisions that deviate from what was initially intended by the producers and consequently what is expected by the users. This raises questions about human control and oversight, so that humans could choose how and whether delegating decision to AI products and systems, to accomplish human-chosen objectives.
- Another essential characteristic of AI-based products and systems is data dependency: data accuracy and relevance is essential to ensure that AI based systems and products take the decisions as intended by the producer. The Union product safety legislation does not explicitly address the risks to safety derived from faulty data. However, according to the “use” of the product, producers should anticipate during the design and testing phases the data accuracy and its relevance for safety functions.
- Additional risks are those stemming from the complexity of the products and systems, as various components, devices and products can be integrated and have influence on each other’s functioning (e.g. products part of a smart home ecosystem). In particular, when the producer carries out the risk assessment of the product, he must consider the intended use, foreseeable use and, where applicable, reasonably foreseeable misuse. In this context, if the producer envisages that their device will be interconnected and will interact with other devices, this should be considered during the risk assessment. Use or misuses are determined on the basis of, for example, experience of past use of the same type of product, accident investigations or human behaviour.
- Emerging digital technologies are affected by complex value chains, too: this is the case for example of products such as computers, service robots, or transport systems. Under the Union product safety framework, no matter how complex the value chain is, the responsibility for

the safety of the product remains with the producer that places the product on the market. Producers are responsible for the safety of the final product including the parts integrated in the product e.g. the software of a computer.

- Finally, the openness to updates and upgrades after their placement on the market. The vast amounts of data involved, the reliance on algorithms and the opacity of AI decision-making make it more difficult to predict the behaviour of an AI-enabled product and to understand the potential causes of damage as well as the combined exposure to cyber-threats.

As seen, the emergence of new digital technologies like AI, the IoT and robotics raise new challenges in terms of product safety and liability.

While in principle the existing Union and national applicable laws are able to cope with emerging technologies, the dimension and combined effect of the challenges of AI could make it more difficult to offer compensation in all cases where this would be justified. Thus, the allocation of the cost when damage occurs may be unfair or inefficient under the current rules. To rectify this and address potential uncertainties in the existing framework, certain adjustments to the Product Liability Directive and national liability regimes through appropriate EU initiatives could be considered on a targeted, risk-based approach, i.e. taking into account that different AI applications pose different risks.

So actually, as reported by an important commenter, “whether this approach achieves the stated aims of fostering innovation and creating an ecosystem of trust is clearly a challenge and an opportunity for pro-active and strategic contributions by all stakeholders”.

Source: European Commission – Report to the European Parliament, the Council and the European Economic and Social Committee.

Link: https://ec.europa.eu/info/sites/info/files/report-safety-liability-artificial-intelligence-feb2020_en.pdf.