BUILDING A DATA ECONOMY WORKSHOP MERGING CHALLENGES IN THE EUROPEAN DATA ECONOMY

In the context of the forthcoming Free Flow of Data package, DG JUST (unit A2 Contract law) and DG CNECT (units G1 Data Policy and Innovation and E4 Internet of Things) organised a 2-day workshop to discuss legal challenges in relation to the access to industrial data and liability. The workshop was also a peer review exercise with different stakeholders (industry, umbrella associations, academics and lawyers) in respect to preliminary findings of a supporting (JUST/CNECT) study examining emerging issues of data ownership, interoperability, (re)usability and access to data, and liability.

- **Day 1 - Access to/transfer of data**

Day 1 examined data-based business models, contractual restrictions and access to data solutions. There was a shared feeling that uncertainties in the legal status of industrial data impact the extent of data flows. Reluctance in data sharing has different reasons. Companies may ignore the conditions under which they can share data (e.g. small start-ups sometimes get data by infringing data protection or IP rights). Major companies have concerns about cybersecurity attacks and privacy breaches as there is often a mix of technical and personal data. Possible disclosure of know-how to competitors is also nourishing a potential reluctance in sharing data with third parties. Building trust thus becomes key when deciding with which third parties to share, and especially which data should be traded. It was also argued that companies should be given incentives to share their data, which would support the development of innovative services related to data.

For many participants data should belong to the data producer/originator (i.e. user of the car/machine collecting data via sensors); some argued that control over data should be granted to the owner of the physical asset. However, participants disagreed on the actual functioning of certain data markets. One example refers to real time vehicle data, access to which seems to be a matter of longstanding contention between the automotive manufacturers and the independent secondary markets (car repair and maintenance). The latter category deplored lack of access to needed data (as data flow takes place between the vehicle and the car producer only via Internet/GPS). They called for EU rules on access to data and asked for guidance/clarification for the relationship between the primary and secondary markets (when data withheld by a primary market is actually needed for services provided by the secondary market operators). A similar scenario seems to arise in other secondary markets (ICT). Insurance providers saw access to data essential for calculating risks (important for the automated cars scenarios.

Many participants supported a sectorial approach, through the **segmentation of the types of data and markets**. Virtually all manufacturers highlighted the importance of freedom of contract and the need for flexible frameworks and contracts to allow return on investment when sharing data. According to telecom providers and manufacturers, few problems arise when access is granted via bilateral relations, but with the IoT, featuring many players, there is uncertainty. Enhanced legal certainty when partnering with more players (especially across border) is needed also because judicial control of terms and conditions is higher in some MS.

On a possible regulatory intervention industry participants were careful. Big industry and telecom providers feared that premature regulation is not a future-proof approach. They asked for clear evidence of market failures or imbalances. Best practices or voluntary schemes would be welcomed.

- **Day 2 - Liability in IoT and robotics**

Challenges for liability in the context of the Internet of Things (IoT) and robotics technology have been discussed during day 2. Identifying liability challenges and clarifying applicable rules are needed for building trust in IoT/robotics technologies. The Commission aims at a single market for the IoT supported by a stable legal framework to incentivise investment and provide legal certainty.

A need for better clarification at conceptual level emerged. Participants supported clear distinctions between IoT and robotics, between categories of robots, between connected and automated cars. Participants agreed in classifying robots along functionality (rather than autonomy) criteria but the appropriate level for classification is to be determined (legislator, standardization bodies, insurance companies). A need of a classification scheme emerged in respect to the IoT.

Some industry participants (software business) argued that neither IoT raises new issues, nor robotics entirely challenges traditional concepts (except for fully autonomous driving). In this opinion, the intrinsic complexity in the IoT can be managed by current rules. However, many participants agreed upon a paradigm shift in relation to product liability. Sales law rules and product liability rules are in place, but not sufficiently addressing situations when things go wrong in IoT/robotics due to software/data services/connectivity failures. One may need to consider whether to bring manufactures of software in the scope of the product liability framework. It was argued that traditional delineation between contractual and extra-contractual liability is challenged by the hybrid reality of IoT/robotics - one may need to rethink liability in a combined way to avoid legal uncertainty.
Some participants highlighted that the IoT and robotics challenge current rules as the digital layer is not properly taken into account - what emerges is, in the end, a services market. In respect to the assumption that a human is always involved in the supply chain, that may not always be the case as the M2M sector is growing due to self-learning algorithms and robots. Although less emphasis has been placed on the autonomy of robots/independent behaviour, certain participants made it clear that some robots could be considered as autonomous agents. Software designers may not be able to foresee all conceivable outcomes of interactions between artificial agents and humans.

The need to enable at the EU level the testing of robots was widely welcomed. Companies face difficulties in testing robots at national level so support or intervention was welcomed. Procedural aspects, as measures flanking substantial issues, were mentioned (i.e. breach notifications and setting up requirement of data sharing for evidential purposes, coupled with burden of proof allocation rules).

As to the liability solutions, different approaches may be envisaged. There is a need to avoid cases where liability may not be attributed to someone. Some saw the need of revisiting product liability rules, other would draw inspiration from risk-opening solutions (taking as an example liability for behaviour of animals) while others favoured new approaches (such as risk-management solutions assigning liability to the person/market actors which is best placed to avoid and minimize costs. It was claimed that strict liability may not necessarily lead to, or incentivize, higher safety. Some industry representatives opposed a joint liability solution as potentially exposing the value chain to greater risks of information disclosure (i.e. cybersecurity aspects).
The EP draft report on civil law rules for robotics was touched upon. Industry and insurance representatives met with scepticism the idea advocated by the report of assigning legal personality to robots and creating a compensation fund. However it was argued that this idea (whether legal personality for robots is a valid legal solution) should be separated from the main discussion - which remains relevant - of having clear adapted rules when the determination of liability in IoT and robotics is not anymore possible due to the ecosystem’s complexity.

Within the EU, in the absence of testing, there is little understanding about the risks and damages that can occur in IoT and robotics. The lack of data on risks and accidents affects the insurers in their ability to calculate and price risks and develop adequate insurance policies. Insurance providers generally took a cautious approach. For the car sector, the motor insurance directive provides for a compulsory insurance scheme to adequately compensate victims. It functions well since this is a mature market, risks being understood. This does not necessarily mean that a compulsory insurance solution might automatically work for all IoT/robotics. Insurers are prepared to insure only risks they can understand. Access to data becomes vital. Only based on data, they can assess risks and calculate premiums. Insurers are currently discussing the type of needed data for automated cars. Some would extend the current product liability rules to robotics, as they could not imagine a situation where, in the light of the technological state of art, liability rules would not help solving problems.