Francesca Gennari

RAILS Blog published 17 June 2022

Liability for IoT Standards in the EU. 'And yet it moves'?

Businesses all over the world consider standards essential enablers of technological development. Standards are sets of processes that allow to build products in the most efficient and, hopefully, safe way. From a decision-making point of view, standards represent the consensus of a precise group of stakeholders on what it takes for a product to be considered 'state of the art'. These considerations also apply to the Internet of Things (IoT), a technology based on sensors incorporated in objects connected to cloud spaces. If standards do not work as they should private law issues will arise. Imagine that a manufacturer of a IoT object applies a standard that is considered state of the art from the major stake-holders in its field. Imagine damage happens because of the application of this standard and, as a consequence, people are severely injured. Think further and make the hypothesis that through a legal action it is ascertained that the standard caused the object to malfunction. Who is to be considered liable? The aim of this blogpost is to investigate the slow evolution of the IoT standards liability debate within Member States (MS) by considering also the Data Act, one of the most recent EU proposed regulations applicable to the IoT.

Standard developing organisations and more

Recently, there has been a rapid increase in the production of IoT standards which can concern access, connectivity, interoperability, cybersecurity and data protection. Generally, there are specialised organisations which create standards, called Standard Developing Organisations (SDOs). At the moment it is possible to regroup SDOs in three main groups depending on their origin: international, regional and national. As far as the EU is concerned, the main regional SDOs are ETSI, CEN and CENELEC. The most known international SDOs are ISO, ITU and IEEE, which is more professionally oriented. Moreover, sometimes a business creates a successful standard that becomes in practice the most used, a *de facto* standard. Whenever SDOs are collective entities, their preferred modality of work is to elaborate the standards within expert groups, but it is quite difficult to understand who is in these groups and how it is possible to have access to meetings minutes without being a group member.
In addition to SDOs, there are other bodies in the EU that try to clarify the extent and the types of different IoT standards, with two main functions. The first reason is to give uniform instructions on safety issues for the IoT, in connection with cybersecurity concerns, which is what ENISA, the EU cybersecurity agency, has been doing recently. The second reason is that the EU Commission backs up and directly or indirectly helps to systematise the number of standards in this field, as most stake-holders feel that there needs to be a better coordination among existing standards more than inventing new ones. As an example, there is a

series of previous initiatives on achieving clarity and interoperability of cloud standards but also the more recent Preliminary Report of the Sector Inquiry into the Consumer Internet of Things. This last document in particular had a whole series of tables illustrating Intellectual Property Rights (IPR) policies to expect, especially when asking a Fair, Reasonable And Non-Discriminatory (FRAND) license for the implementation of a Standard Essential Patent (SEP), which is an intellectual property right (a patent) deemed fundamental for the development of a technological standard.

Legal consequences of defective IoT standards.

The majority of these standards are not legally binding unless they are incorporated in a national legislative act. Hence, if design defect of international non-binding SDO standard is the ultimate source of personal injury, death or property damage the victim would need to use MS rules on tort liability in the absence of a contractual relationship to make a claim. Producers would also be put in similar situations, if they used the standard, to try to recover compensation from the SDO. Some countries such as France might be in favour of an "extended" regress action for the producer, given their consumer protective legal tradition, but others, such as Germany or the UK, might be more restrictive, especially if the damage is purely economic. In the US, this example would be considered too remote to even have legal standing, meaning to be legitimised to bring a legal action to court.
However, in the EU there are also harmonised standards. As a consequence of the New Legislative Framework, building on the previous New Approach, the Commission might task European SDOs (such as ETSI, CEN, CENELEC) to develop standards following its broad indications according to Regulation EU/2012/1025. Once the standard is published into the Official Journal, the Court of Justice of the EU (CJEU) has competence over it, as established in the 2014 judgment *James Elliott Construction*, C-613/14. What are the legal consequences if a harmonised standard is not safe enough? Can the EU Commission be considered at fault because of its delegated power to SDOs or can European SDOs respond for negligence, if that were the case? The court did not answer these questions directly, although Article 340 TFEU states that the EU is liable both under contract and tort liability.
These issues might sound hypothetical, but the importance of standards is growing in digital regulation proposals and we cannot afford accountability nor liability loopholes: new technologies such as the IoT could potentially cause damages to a relevant number of EU citizens. The proposed Data Act regulation values standards, as well as the proposed Artificial Intelligence Act (AIA). In Chapter VIII on interoperability of cloud standards, Article 29 (4) of the Data Act states that "[t]*he Commission may, in accordance with Article 10 of Regulation (EU) No 1025/2012, request one or more European standardisation organisations to draft European standards applicable to specific service types of data processing services*". Could article 340 TFEU be used against the Commission by a IoT producer in case of a defective harmonised standard involving data processing, as this is likely to be the main source of harm caused by IoT objects? The CJEU case law on *locus standi* of legal and physical people

has always been quite restrictive as in the *Plaumann* case, C-25/62. Today, it would be safer to use Article 267 TFEU, the preliminary reference procedure, in order to find the Commission eventually liable together with the MS which implemented the standard. Another partial solution could be available if the Product Liability Directive update would establish that a product is also made of incorporated software, which could be considered a part of a defective good, as it was suggested by the European Law Institute to make it coherent with Directive EU/2019/771 on the sale of digital goods. If that were the case, defects of the physical products standards could be easier to prove. However, this would leave out the standards involved in the cloud, the most external and distant layer from the IoT object and still the most relevant in terms of processing data.

Preliminary conclusions

In this blogpost I tried to highlight the growing importance of standards liability issues in the EU. It is a relevant problem because of the growing importance of standards, not only for the regulation and the proper functioning of IoT but also because proposals of new legislative acts, such as the Data Act, mention them but do not clearly set out which remedies EU citizens have in case of harm resulting from them.
At the moment, liability issues for international defective standards could be covered by MS tort law if the standard is not-binding. With harmonised standards, the CJEU is competent but the *locus standi* requirements to have direct access have been seldom met in the past. The proposed Data Act in its current form mentions the competence for the Commission to set the basis for harmonised rules on processing standards. It is unclear whether this means that the Commission is indirectly 'taking the hit' for eventual mistakes in the development of these standards, or whether it is counting on national rules to develop ways to make SDOs accountable. As a reaction, European SDOs might take out civil liability insurance schemes, as the Notified Bodies must do according to the Medical Devices Regulation, EU/2017/745 (Annex VII, 1.4,1-2). Even if much more needs to be done in terms of liability rules, slowly but surely, there is an ongoing and incremental harmonisation of IoT standards remedies. Whether this actually is an indirect and, perhaps, almost casual consequence of the proposed Data Act, is yet to be seen. In any case, this process is bound to start a discussion about the EU competence over the liability rules applicable to these issues, unless Article 114 TFEU, allowing the harmonisation of the Internal Market, is used as a legal basis to establish EU competence in these matters yet again.

Acknowledgement
This project has received funding from the European Union's Horizon 2020 research and innovation programme under the Marie Skłodowska-Curie ITN EJD grant agreement No 814177