

DOI 10.5817/MUJLT2021-2-1

## STANDARD SETTING ORGANISATIONS FOR THE IOT: HOW TO ENSURE A BETTER DEGREE OF LIABILITY?<sup>1</sup>

by

FRANCESCA GENNARI\*

*This early stage research article outlines an issue that will most likely become more and more important in the upcoming years: the liability regime applicable to the Internet of Things (IoT) objects. In particular, this article will analyse in more detail the liability for defective international interoperability standards. ICT standards include more and more patents that are essential to the development of the standard itself (Standard Essential Patents, SEPs). The producers of ICT standards are generally non-profit and international private organisations with either a European or an international outreach. They have not been considered liable for defective standards so far according to private law rules. The article will use a broad notion of liability, encompassing both accountability and responsibility, in order to map out the main Standard Setting Organisations (SSOs) in the EU with reference to the IoT. Furthermore, the article will assess whether the actual status quo concerning private law liability arising from defective standards needs to change or not.*

### KEY WORDS

*IoT, Standards, Smart-House, Liability, SEP, SSOs, SDOs*

---

<sup>1</sup> 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.

\* Francesca Gennari, PhD student, Law Science and Technology Joint Doctorate, Rights of the Internet of Everything (LAST-JD RIoE), Mykolas Romeris University – University of Bologna – University of Turin, email: frgennari@stud.mruni.eu/francesca.gennari8@unibo.it.

## 1. INTRODUCTION

Our life is standardised. Not only metaphorically, but also practically. Standards are rules, know-how to produce objects that improve efficiency and that guarantee a sufficient security level for our daily life. Among the set of objects that can be interested by standards, legal scholars have focussed on the standards affecting the ICT industry. This field of study showed a deep correlation between traditional Intellectual Property (IP) law (as especially patents, but also know-how and trademarks are involved) and competition law, as the market power in the innovation field is nowadays more and more connected to the IP rights that a company owns. Standard Setting Organizations (SSOs or Standard developing organisations, SDOs)<sup>2</sup> traditionally set these standards but also single companies, consortia and open source standard organisations (OSS) have acquired a standard developing/setting function lately.

The scope of this article is to investigate which kind of liability the creators of ICT standards might incur whenever they create standards for the Internet of Things (IoT) for the household. This particular field of IT innovation has been chosen as it has been receiving constant funding over the last years<sup>3</sup> but also because it is bound to be one of the most widespread applications of IoT technology among consumers<sup>4</sup> and is sufficiently adaptable to possibly mix with more refined and pervasive technologies such as Edge Computing or AI<sup>5</sup>. Moreover, the divide between health and domestic IoT is already blurred. Especially consumer wearables (such as smartwatches or smartphones) already have 'health functions' and, most probably, even after the COVID-19 pandemic ends, most physical and psychological therapy will be done directly from our own homes. In this respect, it is key that the allocation of liability is clear for all the stakeholders involved.

The structure of this early stage research article is the following. Firstly, there will be a review of the state of the art, with a focus

<sup>2</sup> We will use the terms SSOs and SDOs with the same meaning throughout the article.

<sup>3</sup> Nativi, S. et al. (2020) *IoT 2.0 and the INTERNET of TRANSFORMATION (Web of Things and Digital Twins) a multi-facets analysis*. [online] Luxembourg: JRC. Available from: [https://publications.jrc.ec.europa.eu/repository/bitstream/JRC120372/jrc120372\\_report\\_on\\_iot\\_%2815\\_sep\\_2020%29\\_ver\\_3.7.1.pdf](https://publications.jrc.ec.europa.eu/repository/bitstream/JRC120372/jrc120372_report_on_iot_%2815_sep_2020%29_ver_3.7.1.pdf) [Accessed 10 May 2021] p. 46.

<sup>4</sup> Weber, R. (2017) Liability in the Internet of Things. *Journal of Consumer and Market Law*, 6(5), pp. 207-212.

<sup>5</sup> Huh, J., Seo, Y. (2019) Understanding Edge Computing: Engineering Evolution With Artificial Intelligence, *IEEE Access*, pp. 164229-164245.

on the characteristics of IoT home standards and the organisations which create them (2). The main question is whether there is a need for some kind of liability for SSOs. Consequently, if the first answer is affirmative, I will explore which changes to the actual system are possible. In the case the answer is negative, I will examine whether the current system could be further improved and how (3). In order to achieve these results, the explanation of the methodology to apply will be essential (4). This will lead to analyse the characteristics of the most relevant SSOs in the home IoT interoperability field (5). There will be an explanation of the possible paths forward (6) and, finally, some concluding remarks of this initial phase of research.

## 2. STATE OF THE ART. STANDARDS, SSOs AND THE IoT HOUSE

Generally, when talking about standards, we refer to

*"[...] those particular technical specifications developed by a certain set of large, well-established standards organisations [...]"*<sup>6</sup>.

Even more than general standards, ICT standards have a vital economic function as they foster progress in creating more efficient and interoperable components of new technological objects. However, they can also constitute a barrier to enter the market, especially if the standard is based on patented inventions that are considered essential for its development. These patents are called Standard Essential Patents (SEPs). For years, economists and legal scholars have debated about some specific hindrances to the market caused by SEPs. We are referring to patent thickets and patent hold-ups<sup>7</sup>. There are several legal remedies to help create a level playing field for the different operators: Fair, Reasonable and Non-Discriminatory licenses (FRAND)<sup>8</sup>, but also alternative dispute resolution systems<sup>9</sup> or traditional litigation under IP and competition law grounds.

<sup>6</sup> Kurgonaitė, E., Treacy, P. and Bond, E. (2020) Looking Back to the Future—Selective SEP Licensing Through a Competition Law Lens?, *Journal of European Competition Law & Practice*, 11(3-4) pp.133-146. Biddle, C. (2017) No standard for standards: Understanding the ICT standards-development ecosystem. In: Jorge Contreras (ed.). *The Cambridge Handbook of Technical Standardization Law: Competition, Antitrust, and Patents*, 1st ed. Cambridge: Cambridge University Press, p. 19.

<sup>7</sup> Shapiro, C. (2005) Navigating the Patent Thicket: Cross Licenses, Patent Pools and Standard-Setting. *Innovation policy and the Economy*, 1, pp. 119-150. Farrel, J., et al. (2007) Standard Setting, Patents, Hold-Up. *Antitrust Law Journal*, 74 pp. 603-760. Against this theory of the patent hold-up see Galetovic, A. and Haber S., (2017) The fallacies of patent-holdup theory. *Journal of Competition Law and Economics*, 13(1), pp. 1-44.

European law scholarship has not yet explored in detail whether the (mostly) international and private actors that constitute the SSOs<sup>10</sup> are liable under private law rules for creating an IT standard which is defective for using patents that are not essential to its creation. This aspect is particularly worth investigating in the creation of the Internet of Things (IoT), and particularly of the smart home. A smart home can be defined as a

*“[...] home that is automated, via the application of the IoT paradigm and capable of reacting to the requirements of its inhabitants, providing comfort and security”<sup>11</sup>.*

If IoT technology allows to connect objects to other objects, and objects to people thanks to a perception layer that favours human-object and object-object interaction<sup>12</sup>, the human being plays a bigger role in the evolution and performance of these objects than before. Therefore, we have to take into account the human variable while developing this technology and its standards.

What makes the home IoT standards different from other IoT objects is that these objects are directed mostly to consumers<sup>13</sup>. Despite home IoT objects for the house are several and have different functions, the one common characteristic of these objects is that they are multi-layered. These devices contain a physical part (hardware that is bound to be linked to security and safety standards, patents and know-how) and software. The device is connected to a cloud layer<sup>14</sup> (and eventually a fog layer before that) through a gateway within the same house. The variety of damages

---

<sup>8</sup> Kurgonaitė, E., Treacy, P. and Bond, E. (2020) Looking Back to the Future—Selective SEP Licensing Through a Competition Law Lens?. *Journal of European Competition Law & Practice*, 11(3-4) pp.133-146. Picht, P. (2017) Unwired Planet v. Huawei: a Seminal SEP/FRAND decision from the UK. *Journal of Intellectual Property Law & Practice*. 12 (10), October 2017, pp. 867-880.

<sup>9</sup> Contreras, J. and Newman D. (2017) Alternative Dispute Resolution and FRAND Disputes. In: Jorge Contreras (ed.) *The Cambridge Handbook of Technical Standardization Law: Competition, Antitrust, and Patents*, 1st ed., Cambridge: Cambridge University Press, pp. 351-361.

<sup>10</sup> In this group we include, momentarily, not only traditional SDOs, but also consortia, single promoters and Open Source Software organisations (OSS).

<sup>11</sup> Ali, B. and Awad, A. (2018) Cyber and Physical Security Vulnerability Assessment for IoT-based smart homes. *Sensors*, 18(3), p. 817 and ff.

<sup>12</sup> Bandhiopadyay, D. and Sen, J. (2011) Internet of Things: Applications and challenges in technology standardization. *Wireless Personal Communications*, 1, pp. 49-69.

<sup>13</sup> Weber, R. (2017) Liability in the Internet of Things. *Journal of Consumer and Market Law*, 6(5), pp. 207-212.

<sup>14</sup> Ali, B. and Awad, A. (2018), Cyber and Physical Security Vulnerability Assessment for IoT-based smart homes. *Sensors*, 18(3), p. 817.

created by these objects is still under review and partly unclear<sup>15</sup>, but the focus of this article is how the standard could contribute to the damage and not the damage itself.

It is problematic that standards elaborated by SSOs are not law *per se*. They are as influential as the SSOs which create them can be, but they do not generally have a legal binding power. It is then up to the States or transnational organisations such as the EU to decide whether to consider these standards as technical specifications and, therefore, binding, or just as rules whose compliance is not mandatory, although encouraged<sup>16</sup>. Home IoT standards make no exception to this rule.

In the US, despite a history of litigation on the grounds of tortious liability over standard regulations of various kinds, SSOs were always exempted from liability on different grounds, such as a weak link in the causality chain, but also policy and reputational concerns<sup>17</sup>. In line with this approach, I will refer to the liability of classification societies<sup>18</sup> as an enlightening example, because some of the issues studied in this field are similar to those concerning the liability regimes of the SSOs. Classification societies are private owned organisations which certify that ships and vessels are well built and sufficiently secure to sail. In a way, they are similar to ICT SSOs as they are private organisations, but they can have public functions as well. This happens whenever a Public Administration delegates audits functions to them, counting on their extremely specialised expertise in these technical matters. Because of the exercise of these public functions, some countries allow them to be completely, partly or not immune as far as tort liability is concerned<sup>19</sup>. This coexistence of private and

---

<sup>15</sup> European Commission (2020), Report on the safety and liability implications of Artificial Intelligence, the Internet of Things and robotics, (COM(2020)64 final) 02 February. Available from: <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52020DC0064&from=en> [Accessed 10 May 2021].

<sup>16</sup> Delimatsis, P. (2019) International trade and technical standardization. In: Jorge Contreras (ed.), *The Cambridge Handbook of Technical Standardization Law: Further Intersections of Public and Private Law*, 1<sup>st</sup> ed. Cambridge: Cambridge University Press, p. 9. For a more EU-focussed outlook on judicial review of harmonised standard is Tovo, C. (2018) Judicial Review of Harmonized Standards: Changing the Paradigms of Legality and Legitimacy of Private Rulemaking under EU law. *Common Market Law Review*, 55, pp. 1187-1216.

<sup>17</sup> Verbruggen, P. (2019) Good Governance of Private Standardization and the Role of Tort Law. *European Private Law Review*, 27(2), pp. 319-352.

<sup>18</sup> Basedow, J. and Wurmnest W. (2005) *Third-Party Liability of Classification societies. a Comparative Perspective*, 1st ed. Berlin-Heidelberg: Springer, 138 p. Lagoni, N. (2007) *The Liability of Classification Societies*, 1st ed. Berlin-Heidelberg: Springer, 377 p.

<sup>19</sup> Ulfbeck, V. and Möllmann, A. (2019) Public Function Liability of Classification Societies In: Peter Rott (ed.) *Certification-Trust, Accountability and Liability, Studies in European Economic Law and Regulation*, 16, Switzerland: Springer Nature, pp. 210-229.

public function is no stranger to some national scale SSOs (also for technology) in which private stake-holders have a relevant say, together with national governments, in deciding whether a standard must or must not become part of a compulsory technical regulation. However, unlike the ICT SSOs considered in this article, which are mostly international companies, classification agencies do expect to be paid for their certification services. Common law judges have consistently stated that classification societies are not liable if the damage consists of a pure economic loss, whereas that is not always the case when damages involve people<sup>20</sup>. In civil law countries there is a more nuanced approach to the 'private function' liability of classification societies: whenever there is a legal theory that allows third parties to get compensation (i.e. the contract with protective effects against third parties in Germany) the classification society can be liable for negligence in the release of the certification in certain cases<sup>21</sup>. In the same way, one can hold the classification societies accountable under tort law, in compliance with the national tort rules if a private kind of liability is involved<sup>22</sup>. The relevance of the example of classification societies in this context is that they are, such as the SSOs, international organisations or private companies, which are well-known worldwide and whose function is to create trust in objects that might cause damages to whoever uses them. This is done through audits, certification and standardisation procedures.

In the EU, standard litigation concerning products arose with respect of safety standards in the context of the implementation of the so called 'New Approach':

*"[...] where private actors are invited into and given formal responsibilities in both the development and the enforcement of legal standards"* <sup>23</sup>.

In *Fra.bo* (C-171/11) and *Peter Paul* (C-222/02)<sup>24</sup> cases, the Court of Justice of the European Union (CJEU) held *'[...] that public interest reasons can be*

<sup>20</sup> Basedow, J. and Wurmnest W. (2005) *Third-Party Liability of Classification societies. a Comparative Perspective*, 1st ed. Berlin-Heidelberg: Springer, 138 p. Lagoni, N. (2007) *The Liability of Classification Societies*, 1st ed. Berlin-Heidelberg: Springer, p. 38.

<sup>21</sup> Basedow J. and Wurmnest (2005) *op. cit.* p. 101.

<sup>22</sup> Basedow J. and Wurmnest (2005) *op. cit.* p. 102.

<sup>23</sup> Wallerman, A. (2018), Pie in the sky when you die? Civil liability of notified bodies under the Medical Devices Directive: Schmitt. *Common Market Law Review*, 55, p. 265.

<sup>24</sup> Judgment of 12 July 2012, *Fra.bo*, C-171/11, ECLI:EU:C:2012:453; Judgment of 12 October 2004, *Peter Paul*, C- 222/02, ECLI:EU:C:2004:606, as cited by Wallerman A. (2018) *op.cit.*, pp. 270-273.

applied to private standards', but, at the same time, the 'protective purpose' of a certain legislative act (that makes also reference to standards) does not 'entail the conferral of rights upon those who are intended to be protected'<sup>25</sup>. These remarks are even more interesting if these two judgments are put in connection with the more famous and recent *Schmitt* judgment (C-219/15), as Wallerman suggests<sup>26</sup>. The case involved defective breasts implants made by P.I.P. company in the context of the Medical Devices Directive<sup>27</sup>. In this case, the CJEU was called to judge the possibility for a negligent notified body (NB) to be held liable by the claimant, even though there was no explicit mention of the NB liability in the legislative act. The CJEU stated that NBs could be considered responsible according to the liability theories of the single member states (besides, in this specific case, the tortfeasor, P.I.P. company, had gone bankrupt). This last case is particularly interesting as EU law did not formally incorporate these standards which were part of a more general state of the art for specific health products. However, a notified body (NB), that was entrusted by the EU and the Member State (MS), audited and certified that the standards used by the producer complied with a security obligation which had ultimately to benefit consumers/patients, even though there was not any formal link between the NB and the patients themselves. One of the main reasons to keep SSOs exempt from liability is that the large majority of them works on a voluntary basis, and that SSOs are mostly private and non-profit organisations. Unlike state agencies, they do not directly serve the general interest, which includes consumers' expectations and safety. SSOs mainly work as self-regulating *fora* to find efficient solutions to common problems, thus reducing risks. They also try allocating economic power fairly on different markets, including those involved in the creation of the IoT for the house.

However, IoTs are more complex technological objects than the ones we are traditionally used to, given their increasing automation skills and also

<sup>25</sup> Wallerman, A. (2018) *op.cit.*, p. 273.

<sup>26</sup> Wallerman, A. (2018) *op.cit.*, p. 274 analysing Judgment of the Court of 16 February 2017 Elisabeth Schmitt v TÜV Rheinland LGA Products GmbH, C-219/15, ECLI:EU:C:2017:128.

<sup>27</sup> Council Directive 93/42/EEC of 14 June 1993 concerning medical devices *Official Journal of the European Union (O J L 169)* 12 July 1993. Available from: <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:31993L0042&from=EN> [Accessed 10 May 2021]. To have a clear explanation of the path and the rationale that brought the Directive to become a Regulation and why it can still be improved, see also Rott, P. (2019) Certification of Medical Devices: Lessons from the PIP Scandal. In: Peter Rott (ed.) *Certification-Trust, Accountability and Liability, Studies in European Economic Law and Regulation*, 16, Switzerland: Springer Nature, pp. 189-211.

the capacity to react 'intelligently' to environmental changes. Therefore, it is very important that users and consumers start to trust them and to find them reliable in order for these objects to succeed.

One can reach trustworthiness in technology both through the construction of safer technology, compliant with fundamental rights, and also through the creation of a legal system of liability and remedies that is clear enough for all the stakeholders involved<sup>28</sup>. In order to do that, it is essential to distinguish the characteristics of the stakeholders that are involved in the standardisation process for the home IoT. It is then useful to use a taxonomy for SSOs. Biddle created a taxonomy that is rich and is also the most complete available at the moment (see further 5). It envisages SSOs as a general group that is composed by 'traditional' SDOs and consortia. Important actors in this field are also OSS organisations and single promoters of *de facto* standard<sup>29</sup>. More specifically, Biddle divides the SDOs for IT in different groups. The first one *a*) can be the one of the so called big three (or four) international SDOs. Then there are the *b*) regional SDOs (e.g. the European Committee for standardisation) followed by *c*) national SDOs, made by national bodies or agencies. Furthermore, there are *d*) large private sector-led SDOs (such as the IEEE), *e*) small private sector-led SDOs and *f*) SDOs of SDOs which have important regional and national SDOs as their constituents. However, also consortia's power has not to be underestimated. They can be *a*) incorporated *b*) voluntary or *c*) umbrella consortia<sup>30</sup>. Finally, there are Open Source SSOs which are characterised by more openness, due process and transparency in the decision-making process than private SDOs<sup>31</sup>. Some authors share the view that OSS and traditional SDOs are complementary, and therefore both necessary<sup>32</sup>. However, sometimes it takes just one company (single standard promoter), promoting its *de facto* standard, for the standard to become mainstream and

<sup>28</sup> The compliance with ethics, law and technological robustness are the key principle that will guide the EU in the development of a trustworthy AI. AI-HLEG (2019) *Ethics Guidelines for a Trustworthy AI*. [online] Available from: <https://ec.europa.eu/digital-single-market/en/news/ethics-guidelines-trustworthy-ai> [Accessed 10 May 2021] p. 5.

<sup>29</sup> Biddle, C. (2017) No standard for standards: Understanding the ICT standards-development ecosystem. In: Jorge Contreras (ed). *The Cambridge Handbook of Technical Standardization Law: Competition, Antitrust, and Patents*, 1st ed. Cambridge: Cambridge University Press, pp. 19-24.

<sup>30</sup> Biddle, C. (2017) *ibid.*

<sup>31</sup> Biddle, C. (2017) *ibid.*

<sup>32</sup> Kappos, D. (2019) OSS and SDO: Symbiotic Functions in the Innovation Equation. In: Jorge Contreras, *The Cambridge Handbook of Technical Standardization Law*, 1st ed. Cambridge: Cambridge University Press, pp. 198-202.



widely used<sup>33</sup>. It is noteworthy that some private SDOs are more transparent than others. This is of the utmost importance whenever the standard adopted takes into consideration several SEPs. Practical solutions on how to guarantee a fair judgment regarding a patent's essentiality, which means its indispensability for the creation of a standard, are still difficult to assess when decisions are made with consensus and on the basis of the self-promotion of the inventor<sup>34</sup>. Moreover, from a theoretical point of view, there are still discussions about whether one has to interpret essentiality in the strict technical-IT meaning, which will give way to a more restrictive interpretation, or in its commercial sense, which will allow a wider field of application<sup>35</sup>. For the moment, each SSOs has its own essentiality policy. In any case, the European Commission has launched and supported a series of economic and legal studies in order to understand the extent of the essentiality requirement. In this way there could be a uniform approach to interpret the meaning of essentiality, at least at the EU level<sup>36</sup>.

### 3. RESEARCH QUESTION(S)

In light of the above, the research questions are the following. Suppose a standard turns out to be defective. Is it fair that SSOs are immune from liability for the production of it?

If yes, how to improve this regime? If immunity from liability is unfair, what should be a suitable alternative?

<sup>33</sup> Biddle, C. (2017) No standard for standards: Understanding the ICT standards-development ecosystem. In: Jorge Contreras (ed). *The Cambridge Handbook of Technical Standardization Law: Competition, Antitrust, and Patents*, 1st ed. Cambridge: Cambridge University Press, pp. 19-24.

<sup>34</sup> COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL AND THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE Setting out the EU approach to Standard Essential Patents, COM/2017/0712 final. Available from: <https://eur-lex.europa.eu/legalcontent/EN/TXT/PDF/?uri=CELEX:52017DC0712&qid=1610039668242&from=EN> [Accessed 10 May 2021] p.5. See also Contreras, J. (2019), Essentiality and Standards- Essential Patents. In: Jorge Contreras (ed.), *The Cambridge Handbook of Technical Standardization Law: Competition, Antitrust, and Patents*, 1st ed. Cambridge: Cambridge University Press, pp. 213-230.

<sup>35</sup> Contreras, J. (2019), Essentiality and Standards- Essential Patents. In: Jorge Contreras (ed.), *The Cambridge Handbook of Technical Standardization Law: Competition, Antitrust, and Patents*, 1st ed. Cambridge: Cambridge University Press, pp. 213-230.

<sup>36</sup> See Bekkers, R. et al. (2020) *Pilot Study for Essentiality Assessment of Standard Essential Patents* [online] Luxembourg: JRC. Available from <http://publications.jrc.ec.europa.eu/repository/handle/JRC119894> [Accessed 10 May 2021].

#### 4. METHODOLOGY

Given the wide variety of standards that can be applied to the IoT world, it is indispensable to select the most relevant ones. Interoperability standards are now truly crucial to the home IoT development. In fact, they allow the different objects to communicate and to react not only with the user-consumer but also with the entirety of the home environment. I understand interoperability in an extended sense: namely, as the technical ability to enable communication between smart objects, thus investing all the layers of the domestic IoT, from the physical to the cloud one.

Secondly, liability will be used in a very broad sense. It will encompass both the traditional tort and contractual meaning and broader concepts such as accountability and responsibility. This will also be more in line with a holistic approach to law and technology which is preferable when dealing with new technologies, in order to have a wider selection of *ex ante* and *ex post* remedies<sup>37</sup>. Finally, the investigation will be devoted mainly to the EU scenario as far as home IoT is involved. From a terminological point of view, I will address the humans living the house as users/consumers, because IoT objects serve both kinds of subjects. For the time being, I will not consider that user/consumer to be also a potential data subjects as the discussion with the interrelations about General Data Protection Regulation (GDPR)<sup>38</sup> exceeds the purpose of this article.

#### 5. IoT HOME INTEROPERABILITY SSOs: AN EARLY STAGE CASE STUDY

In order to analyse these SSOs I will use two main schemes. To find out how many SSOs there are in the EU, I will use and integrate the list Nativi et Al. compiled in their most recent report<sup>39</sup>. In order to analyse the characteristics of these SSOs, I will use Biddle's taxonomy as explained in 2. The aim is to understand whether the actual system is transparent and competitive

---

<sup>37</sup> Bakhoun, M. et al. (2018) *Personal Data in Competition, Consumer Protection and Intellectual Property. Towards a Holistic Approach*. Berlin: Springer.

<sup>38</sup> Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). *Official Journal of the European Union* (OJ L 119) 4 May. Available from: <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&qid=1610038683923&from=EN> [Accessed 10 May 2021].

<sup>39</sup> Nativi, S. et al. (2020) *IoT 2.0 and the INTERNET of TRANSFORMATION (Web of Things and Digital Twins) a multi-facets analysis*. [online] Luxembourg: JRC. Available from: [https://publications.jrc.ec.europa.eu/repository/bitstream/JRC120372/jrc120372\\_report\\_on\\_iot\\_%2815\\_sep\\_2020%29\\_ver\\_3.7.1.pdf](https://publications.jrc.ec.europa.eu/repository/bitstream/JRC120372/jrc120372_report_on_iot_%2815_sep_2020%29_ver_3.7.1.pdf) [Accessed 10 May 2021] p. 22.

enough to ensure that necessary SEPs are integrated into future IoT technical standards.

*International government-participated SSOs.* The best known global SSOs for IoT domestic technology are ISO and IEC. They are international organisations in which national standard bodies participate and whose aim is to harmonise standards in different fields, included the one of the IoT. The rules about membership and the identity of the members are clearly explained. In 2020, ISO and IEC created the standard ISO/IEC TR21823-2 which will foster communication and peer to peer connectivity<sup>40</sup>. This standard is available to purchasers. The availability of most of the documents suggests a sufficient level of transparency. However, it is difficult to have access to the repository for Intellectual Property Rights (IPRs) and SEPs. More concentrated on the European market are the two standardisation bodies ETSI and CEN-CENELEC. In particular, ETSI released its standard for Consumer IoT in 2020 (ETSI/EN 303 645) which is intended to increase the cybersecurity level of connected smart devices<sup>41</sup>.

*International (mainly) private SSOs of SSOs.* The Open Connectivity Foundation (OCF) focuses more on the standards concerning how to connect the device and the cloud<sup>42</sup>. International standards of ISO and IEC accepted also OCF specifications<sup>43</sup>. Although its specifications are publicly available, OCFs members are private companies. By perusing the site, the organisational chart is clearly detailed<sup>44</sup>. Furthermore, there is one M2M which unites major ICT SSOs in the world included the European ETSI<sup>45</sup>. Its main effort is to create a 'common service layer'<sup>46</sup> mostly for industrial IoT. Its site provides access to the identity of the members, its

<sup>40</sup> Lewis, B. (2020) *Standard Hat Trick for the Internet of Things*. [online] Geneva: ISO. Available from: <https://www.iso.org/news/ref2529.html> [Accessed 10 May 2021].

<sup>41</sup> ETSI (2020) *Consumer IoT Security*. [online] Sophia-Antipolis: ETSI <https://www.etsi.org/technologies/consumer-iot-security> [Accessed 10 May 2021].

<sup>42</sup> Nativi, S. et al. (2020) *IoT 2.0 and the INTERNET of TRANSFORMATION (Web of Things and Digital Twins) a multi-facets analysis*. [online] Luxembourg: JRC. Available from: [https://publications.jrc.ec.europa.eu/repository/bitstream/JRC120372/jrc120372\\_report\\_on\\_iot\\_%2815\\_sep\\_2020%29\\_ver\\_3.7.1.pdf](https://publications.jrc.ec.europa.eu/repository/bitstream/JRC120372/jrc120372_report_on_iot_%2815_sep_2020%29_ver_3.7.1.pdf) [Accessed 10 May 2021] p. 22.

<sup>43</sup> Nativi, S. et al. (2020), *ibid*.

<sup>44</sup> Open Connectivity foundation (2021) *Open Connectivity Foundation Organizational Structure* [webpage]. Available from: <https://openconnectivity.org/foundation/organizational-structure/> [Accessed 10 May 2021].

<sup>45</sup> Nativi, S. et al. (2020) *IoT 2.0 and the INTERNET of TRANSFORMATION (Web of Things and Digital Twins) a multi-facets analysis*. [online] Luxembourg: JRC. Available from: [https://publications.jrc.ec.europa.eu/repository/bitstream/JRC120372/jrc120372\\_report\\_on\\_iot\\_%2815\\_sep\\_2020%29\\_ver\\_3.7.1.pdf](https://publications.jrc.ec.europa.eu/repository/bitstream/JRC120372/jrc120372_report_on_iot_%2815_sep_2020%29_ver_3.7.1.pdf) [Accessed 10 May 2021], pp.22-23.

<sup>46</sup> Nativi S. et al. (2020) *ibid*.

organisational chart and its processes<sup>47</sup>. Finally, there is OMA Spec Works for a connected world<sup>48</sup> which comes from the fusion of IPSO, Open Mobile Alliance and Open Mobile SpecWorks<sup>49</sup>. Its specifications are publicly available on the site. Furthermore, there is the description of the phases of the process to obtain these specifications which adds transparency to the whole process<sup>50</sup>. Although it aims at being 'open', the organisation is private in character.

*International private SSO*: IEEE is a sector led based SSO which produced some interoperability standards for IoT, such as P-1451-99<sup>51</sup>, which will facilitate the object to object communication layer. Furthermore, there is the 'Project Connected Home over IP<sup>52</sup>' which reunites some of the most important tech companies (e.g. Google, Amazon, Ikea). They will use a Zigbee standard in order to create a more connected home. The companies that participate in it are private and, therefore, it can be regarded as a large private voluntary SSO. Given the popularity of some of its participants, it could be that in a few years this SSO can become dominant on the home IoT market. Therefore, transparency about this SSO is essential. At the moment of writing, on the website of the project there is an updated list of participants and a link to Github for the source code that were not present some months ago<sup>53</sup>. It is indeed a positive improvement since the launch of the website in 2019.

*Regional SSOs*. In the EU, AIOTI, which is the acronym for the Alliance for Internet of Things Innovation<sup>54</sup>, is a regional SSO with some features of an OSS. The EU Commission created it in 2015 and it is a mixed regional SSO with private and public members. Its mission is to eliminate standard

<sup>47</sup> one M2M (2017) *one M2M* [webpage] Available from: <https://www.onem2m.org/> [Accessed 10 May 2021].

<sup>48</sup> Oma SpecWorks (2021) *OMA SpecWorks* [webpage] Available from: <https://omaspecworks.org/> [Accessed 10 May 2021].

<sup>49</sup> Nativi, S. et al. (2020) *IoT 2.0 and the INTERNET of TRANSFORMATION (Web of Things and Digital Twins) a multi-facets analysis*. [online] Luxembourg: JRC. Available from: [https://publications.jrc.ec.europa.eu/repository/bitstream/JRC120372/jrc120372\\_report\\_on\\_iot\\_%2815\\_sep\\_2020%29\\_ver\\_3.7.1.pdf](https://publications.jrc.ec.europa.eu/repository/bitstream/JRC120372/jrc120372_report_on_iot_%2815_sep_2020%29_ver_3.7.1.pdf) [Accessed 10 May 2021], p. 24.

<sup>50</sup> Nativi S. et al. (2020) *op.cit.*, p. 23.

<sup>51</sup> IEEE Standards (2020) *Standard for Harmonization of the Internet of Things (IoT)* [webpage]. Available from: <https://standards.ieee.org/project/1451-99.html> [Accessed 10 May 2021].

<sup>52</sup> Nativi, S. et al. (2020) *op.cit.*, pp. 22-24.

<sup>53</sup> Connected home over IP (2020) *Connected home over IP* [website]. Available from <https://www.connectedhomeip.com/> [Accessed 10 May 2021].

<sup>54</sup> Nativi, S. et al. (2020), *IoT 2.0 and the INTERNET of TRANSFORMATION (Web of Things and Digital Twins) a multi-facets analysis*. [online] Luxembourg: JRC. Available from: [https://publications.jrc.ec.europa.eu/repository/bitstream/JRC120372/jrc120372\\_report\\_on\\_iot\\_%2815\\_sep\\_2020%29\\_ver\\_3.7.1.pdf](https://publications.jrc.ec.europa.eu/repository/bitstream/JRC120372/jrc120372_report_on_iot_%2815_sep_2020%29_ver_3.7.1.pdf) [Accessed 10 May 2021], pp. 22-23.

gaps in IoT standards<sup>55</sup>. It is divided in working groups and collaborates with other regional organisations and with international standardisations bodies<sup>56</sup>.

*The only private but open stand-alone promoter* which will have an influence in Europe is Mozilla IoT and Web of things<sup>57</sup>. Mozilla can be considered a single promoter standard setting actor that is privacy driven<sup>58</sup>. Looking through the website, it is interesting to note that the main objective

*"[...] is to create a decentralized IoT by giving things URLs on the web to make them linkable and discoverable and defining a standard data model and APIs and make them interoperable [...]"*<sup>59</sup>.

Overall, most of these SSOs have either a global or a more European outreach; working in groups is the most efficient way to create standards but one could improve the levels of transparency as far as IPRs and SEPs are concerned. If any of these SSOs creates a defective standard which is incorporated in a IoT home product, at the moment, a part from national tort liability rules, there are no other legal means for users-consumers, unless a broad interpretation of the Product Liability Directive (PLD) prevails, as well as a wide definition of the concept of defect in Article 1 and 6, 1) of the PLD, concerning the level of security and defectiveness of the product<sup>60</sup>. If this happens, the IoT manufacturer could use the risk-development exception contained in Article 7, c) of the PLD. This exception consists in the justification that the state of the art of science and technical development at the time of the creation/commercialisation of the product was not as advanced so as to prevent the product from causing damage. However, the possibility of exemption from this kind of strict liability varies considerably in the EU because there are different legal traditions: national

<sup>55</sup> Nativi, S. et al. (2020) *ibid.*

<sup>56</sup> AIOTI, (2018) *AIOTI* [webpage]. Available from: <https://aioti.eu/structure/collaborations/> [Accessed 10 May 2021].

<sup>57</sup> Nativi S. et al. (2020) *op.cit.* p. 24.

<sup>58</sup> Nativi S. et al. (2020) *ibid.*

<sup>59</sup> Mozilla Web of Things (2018) *Mozilla Web Things* [webpage] Available from: <https://iot.mozilla.org/about/> [Accessed 10 May 2021]

<sup>60</sup> Council Directive 85/374/EEC of 25 July 1985 on the approximation of the laws, regulations and administrative provisions of the Member States concerning liability for defective products *Official Journal of the European Union* (O J L 210) 7 August. Available from <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:31985L0374&from=EN> [Accessed 10 May 2021].

judges tend to share different views on the extent of consumers' protection<sup>61</sup>.

## 6. POSSIBLE PATHS FORWARD

At the moment there is no case brought before the CJEU that illustrates how a defective standard might have affected the functioning of a home IoT object, maybe because potential claimants do not yet know that a damage occurs due to a defective standard, or maybe because it is not worth it or not possible to go to court. It can also be the case that the lack of SSOs liability is satisfactory and economically convenient for the producers involved in this process. Certainly, until today this system mainly relies on the interaction between competition and IP law. The remedies of both these different legal fields have worked, but at a price: only innovators and exploiters as direct and indirect market competitors were involved, whereas users-consumers were not. In order also to achieve a better form of governance of non-state actors in technology, such as SSOs are, a major involvement of the home IoT user will be necessary in the medium-long term.

It is not that difficult to imagine that, because of an interoperability defect in the IoT communication, a material or immaterial damage can take place. In that case, if the IoT manufacturer followed state of the art interoperability protocols and specifications, it would not be fair that he is the only one to be held liable. Even if an EU certification agency for IoT objects is created, taking the best of all the SSOs in this field, it is however unlikely that there will be a creation of an *ad hoc* unique liability system for these objects in the near future.

Despite its competence in steering and designing a framework digital policy, the EU does not have the legal competence to touch upon MS liability systems, not even the ones that involve new technologies such as the IoT. The only limit for MS is that additional liability systems of otherwise EU regulated subjects must not hinder the creation of a Digital Single Market<sup>62</sup>.

---

<sup>61</sup> For instance, France strongly opposed the risk development exception and the PLD in general as it ratified it in 1998, ten years after the date it should have done that enacted according to EU law. See also Larroumet, Ch.(1998) La responsabilité du fait des produits défectueux après la loi du 19 mai 1998, *Recueil Dalloz (D.)*, 33e cahier, chron., p. 311 ; and also Viney, G.(1998), L'introduction en droit français de la directive européenne du 25 juillet 1985 relative à la responsabilité de produits défectueux, *D.*, 31e cahier, chron. p. 23.

<sup>62</sup> See the Judgment of the Court of 25 April 2002, María Victoria González Sánchez v Medicina Asturiana SA. Case C-183/00, ECLI:EU:C:2002:255.

Besides, the P.I.P. case brought before the CJEU shows that EU law will not prevent MS from deciding whether there could be a part of a damage compensation to be paid by an intermediary private body. It could be applicable also when an interoperability standard has sensibly concurred in a damage while the object was normally used. Establishing the correct causality sequence will not be that difficult if, as it seems, the computational power of these objects will increase through edge computing technology and maybe with the help of distributed ledger technologies (DLTs). This will allow to log most of operations in the device and not just in the cloud layer, thus facilitating the possibility to understand how the damage was caused. Whether this hypothetical SSO liability has tortious or contractual nature is an issue that the MS will have to decide, in line with their legal theory history and developments of their contemporary society. The most efficient model would be the one that stake-holders will share the most.

In connection with the broad meaning of liability given in 4, we need *ex ante* measures more connected to soft law starting from today. It is important to clearly outline the organisational structure of all these SSOs: in the list in 5, some SSOs comply with this requirement and some other SSO do not or do not do enough. Furthermore, it will be interesting to understand which companies or institutions take part also in open standard setting organisations, provided that GDPR is respected. The working group division is indeed the most wide-spread way of working on standards. However, some more efforts in order to understand how the procedure to adopt a standard works are needed already. It is not necessary to detail the content of every procedure (the minutes of meetings should be available internally and could be accessed by non-members on the basis of Regulation on Access to Documents<sup>63</sup>, at least in the EU) but it will be helpful if the website showed a synthetic scheme of these procedures. These are not binding legal obligations. However, as already outlined by the European Commission in 2017, they are very important also for assessing the essentiality of SEPs, which can be relevant when setting interoperability standards for the IoT<sup>64</sup>. As already pointed out by the Commission and restated by Commissioner Breton

---

<sup>63</sup> Regulation (EC) No 1049/2001 of the European Parliament and of the Council of 30 May 2001 regarding public access to European Parliament, Council and Commission documents, *Official Journal of the European Union* (O J L 145) 31 May. Available from: <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32001R1049&from=EN> [Accessed 10 May 2021].

recently<sup>65</sup>, a closer collaboration with patents offices in this respect is also desirable<sup>66</sup>. In conclusion, the actual system still works but the changes brought by the home IoT in terms of object-human and object-object interaction are conspicuous and two kinds of actions could be needed in the medium-long term. Firstly, a MS has to assess whether the SSOs can bear some form of liability in case the standard has concurred sensibly in the creation of a material or immaterial damage. It would be preferable to have either a regress action towards an SSO or the joint re-payment of the damage as remedies. As a consequence, these remedies would not only reassure consumers but also do push SSOs to work at the best of their potential. Secondly, some soft law measures are required in order to guarantee process and membership transparency. Despite not being a legal obligation, transparency can help in assessing the eventual liability of the SSOs and to select the best innovations in more traditional IP and competition issues.

## CONCLUSIONS

This early stage study article analysed the topic of liability of SSOs in the home IoT. In order to understand whether the actual system is still efficient as it actually stands, a particular methodology has been used.

Firstly, defective standards concerning interoperability are the focus of the analysis. The motivation about choosing these types of standards is that one of the main features of the home IoT is the interaction between objects and other objects and objects and humans. Furthermore, liability is considered in a broad sense, not only from a tortious or contractual point of view, but also in the sense of accountability of SSOs. This is in line with

---

<sup>64</sup> COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL AND THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE Setting out the EU approach to Standard Essential Patents (COM/2017/0712 final) 29 November. Available from: <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52017DC0712&from=EN> [Accessed 10 May 2021].

<sup>65</sup> COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS Making the most of the EU's innovative potential An intellectual property action plan to support the EU's recovery and resilience, Brussels, (COM(2020) 760 final) 25 November. Available from: <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020DC0760&from=EN> p. 3 [Accessed 10 May 2021].

<sup>66</sup> A wish that has already partly been realised thanks to the collaboration of ETSI and several European Patent Offices and scholars in an experimental study on the essentiality of SEPs. See also Bekkers, R. et al. (2020) *Pilot Study for Essentiality Assessment of Standard Essential Patents* [online] Luxembourg: JRC. Available from <http://publications.jrc.ec.europa.eu/repository/handle/JRC119894> [Accessed 10 May 2021].



the application of a legal holistic approach when analysing new technologies.

The field of investigation has then been further restricted to the EU law and interoperability of SSOs active in the EU. A synthetic case-study showed that the majority of SSOs in the EU consists of mostly sector-led and non-profit organisations whose main difference lies in either a more European or a more global outreach. Competition-wise, it seems to be a dynamic market at the moment but things in digital markets can change quite rapidly and abruptly.

It has then been noted that malfunctioning in the deployment of the interoperability standard can be a concurring or the main cause in the development of a material or immaterial damage in the house. Until now the EU has not established a uniform liability rule over digital technologies yet, because it does not have a clear-cut competence to do so. Nevertheless, MS can implement forms of intermediary liability (as in the P.I.P. case) provided that it does not hinder the creation of the Digital Single Market. The choice for the type of liability (tortious or contractual) will be of the MS, in line with their legal traditions.

These normative steps however are not enough. In compliance with a broad meaning of liability, some transparency and accountability measures could be improved in the SSOs organisational structure. A clearly detailed layout of the organisation, the mention of the participants (private companies and research institutes) together with a closer collaboration with European patent offices to assess whether a patent is really essential to the creation of the standard are good strategies for SSOs both when a litigation over a patent arises and whenever a liability judgment for a defective standard might become a realistic expectation.

## LIST OF REFERENCES

- [1] AI-HLEG (2019) *Ethics Guidelines for a Trustworthy AI*. [online] Available from: <https://ec.europa.eu/digital-single-market/en/news/ethics-guidelines-trustworthy-ai> [Accessed 10 May 2021].
- [2] AIOTI, (2018) *AIOTI* [webpage]. Available from: <https://aioti.eu/structure/collaborations/> [Accessed 10 May 2021].
- [3] Ali, B. and Awad, A. (2018), Cyber and Physical Security Vulnerability Assessment for IoT-based smart homes. *Sensors*, 18(3).

- [4] Bandhiopadhyay, D. and Sen, J. (2011) Internet of Things: Applications and challenges in technology standardization. *Wireless Personal Communications*, 1.
- [5] Bakhoun, M. et al. (2018) *Personal Data in Competition, Consumer Protection and Intellectual Property. Towards a Holistic Approach*. Berlin: Springer.
- [6] Basedow, J. and Wurmnest W. (2005) *Third-Party Liability of Classification societies. a Comparative Perspective*, 1st ed. Berlin-Heidelberg: Springer.
- [7] Bekkers, R. et al. (2020) *Pilot Study for Essentiality Assessment of Standard Essential Patents* [online] Luxembourg: JRC. Available from <http://publications.jrc.ec.europa.eu/repository/handle/JRC119894> [Accessed 07 January 2021].
- [8] Biddle, C. (2017) No standard for standards: Understanding the ICT standards-development ecosystem. In: Jorge Contreras (ed.). *The Cambridge Handbook of Technical Standardization Law: Competition, Antitrust, and Patents*, 1st ed. Cambridge: Cambridge University Press.
- [9] Connected home over IP (2020) *Connected home over IP* [website]. Available from <https://www.connectedhomeip.com/> [Accessed 10 May 2021].
- [10] Contreras, J. (2019), Essentiality and Standards- Essential Patents. In: Jorge Contreras (ed.), *The Cambridge Handbook of Technical Standardization Law: Competition, Antitrust, and Patents*, 1st ed. Cambridge: Cambridge University Press.
- [11] Contreras, J. and Newman D. (2017) Alternative Dispute Resolution and FRAND Disputes. In: Jorge Contreras (ed.) *The Cambridge Handbook of Technical Standardization Law: Competition, Antitrust, and Patents*, 1st ed., Cambridge: Cambridge University Press.
- [12] Council Directive (1993) 93/42/EEC of 14 June 1993 concerning medical devices *Official Journal of the European Union (O J L 169)* 12 July. Available from: <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:31993L0042&from=EN> [Accessed 7 January 2021].
- [13] Council Directive 85/374/EEC of 25 July 1985 on the approximation of the laws, regulations and administrative provisions of the Member States concerning liability for defective products. *Official Journal of the European Union (OJ L 210)* 7 August. Available from <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:31985L0374&from=EN> [Accessed 7 January 2021]) 7 August. Available from <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:31985L0374&from=EN> [Accessed 10 May 2021].

- [14] Delimatsis, P. (2019) International trade and technical standardization. In: Jorge Contreras (ed.), *The Cambridge Handbook of Technical Standardization Law Further Intersections of Public and Private Law*, 1<sup>st</sup> ed. Cambridge: Cambridge University Press.
- [15] ETSI (2020) *Consumer IoT Security*. [online] Sophia-Antipolis: ETSI <https://www.etsi.org/technologies/consumer-iot-security> [Accessed 10 May 2021].
- [16] European Commission: (2020) COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS, Making the most of the EU's innovative potential An intellectual property action plan to support the EU's recovery and resilience, Brussels, (COM (2020) 760 final) 25 November. Available from: <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020DC0760&from=EN> [Accessed 7 January 2020].
- [17] European Commission :(2020), Report on the safety and liability implications of Artificial Intelligence, the Internet of Things and robotics, (COM(2020)64 fina) 02 February. Available from: <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52020DC0064&from=en> [Accessed 10 May 2021].
- [18] European Commission: (2017) COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL AND THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE Setting out the EU approach to Standard Essential Patents (COM/2017/0712 final) 29 November. Available from: <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52017DC0712&from=EN> [Accessed 10 May 2021].
- [19] Farrel, J., et al. (2007) Standard Setting, Patents, Hold-Up. *Antitrust Law Journal*, 74.
- [20] Galetovic, A. and Haber S., (2017) The fallacies of patent-holdup theory. *Journal of Competition Law and Economics*, 13(1).
- [21] Huh, J., Seo, Y. (2019) Understanding Edge Computing: Engineering Evolution With Artificial Intelligence, *IEEE Access*, pp. 164229- 164245.
- [22] IEEE Standards (2020) *Standard for Harmonization of the Internet of Things (IoT)*[webpage]. Available from: <https://standards.ieee.org/project/1451-99.html> [Accessed 10 May 2021].
- [23] Kappos, D. (2019) OSS and SDO: Symbiotic Functions in the Innovation Equation. In: Jorge Contreras, *The Cambridge Handbook of Technical Standardization Law*, 1st ed. Cambridge: Cambridge University Press.
- [24] Kurgonaitė, E., Treacy, P. and Bond, E. (2020) Looking Back to the Future—Selective SEP Licensing Through a Competition Law Lens?, *Journal of European Competition Law & Practice*, 11(3-4).

- [25] Lagoni, N. (2007) *The Liability of Classification Societies*, 1st ed. Berlin-Heidelberg: Springer.
- [26] Larroumet, Ch.(1998) La responsabilité du fait des produits défectueux après la loi du 19 mai 1998, in *Recueil Dalloz (D.)*, 33e cahier, chron.
- [27] Lewis, B. (2020) *Standard Hat Trick for the Internet of Things*. [online] Geneva: ISO. Available from <https://www.iso.org/news/ref2529.html> [Accessed 10 May 2021].
- [28] Mozilla Web of Things (2018) *Mozilla Web Things* [webpage] (Available from: <https://iot.mozilla.org/about/> [Accessed 10 May 2021].
- [29] Nativi, S. et al. (2020) *IoT 2.0 and the INTERNET of TRANSFORMATION (Web of Things and Digital Twins) a multi-facets analysis*, Luxembourg: JRC, Available from: [https://publications.jrc.ec.europa.eu/repository/bitstream/JRC120372/jrc120372\\_report\\_on\\_iiot\\_%2815\\_sep\\_2020%29\\_ver\\_3.7.1.pdf](https://publications.jrc.ec.europa.eu/repository/bitstream/JRC120372/jrc120372_report_on_iiot_%2815_sep_2020%29_ver_3.7.1.pdf).
- [30] Oma SpecWorks (2021) *OMA SpecWorks* [webpage] Available from: <https://omaspecworks.org/> [Accessed 10 May 2020].
- [31] one M2M (2017) *one M2M* [webpage] Available from: <https://www.onem2m.org/> [Accessed 7 January 2021].
- [32] Open Connectivity foundation (2021) *Open Connectivity Foundation Organizational Structure* [webpage] Available from: <https://openconnectivity.org/foundation/organizational-structure/> [Accessed 10 May 2021].
- [33] Picht, P. (2017) Unwired Planet v. Huawei: a Seminal SEP/FRAND decision from the UK. *Journal of Intellectual Property Law & Practice*. 12 (10), October 2017.
- [34] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). *Official Journal of the European Union* (O J L 119) 4 May. Available from: <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&qid=1610038683923&from=EN> [Accessed 10 May 2021].
- [35] Regulation (EU) No 1049/2001 of the European Parliament and of the Council of 30 May 2001 regarding public access to European Parliament, Council and Commission documents, *Official Journal of the European Union* (O J L 145) 31 May. Available from: <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32001R1049&from=EN> [Accessed 10 May 2021].

- [36] Rott, P. (2019) Certification of Medical Devices: Lessons from the PIP Scandal. In: Peter Rott (ed.) *Certification-Trust, Accountability and Liability, Studies in European Economic Law and Regulation*, 16, Switzerland: Springer Nature.
- [37] Shapiro, C. (2005) Navigating the Patent Thicket: Cross Licenses, Patent Pools and Standard-Setting. *Innovation policy and the Economy*, 1.
- [38] Tovo, C. (2018) Judicial Review of Harmonized Standards: Changing the Paradigms of Legality and Legitimacy of Private Rulemaking under EU law *Common Market Law Review*, 55.
- [39] Ulfbeck, V. and Möllmann, A. (2019) Public Function Liability of Classification Societies In: In: Peter Rott (ed.) *Certification-Trust, Accountability and Liability, Studies in European Economic Law and Regulation*, 16, Switzerland: Springer Nature.
- [40] Verbruggen, P. (2019) Good Governance of Private Standardization and the Role of Tort Law. *European Private Law Review*, 27(2).
- [41] Viney, G. (1998), L'introduction en droit français de la directive européenne du 25 juillet 1985 relative à la responsabilité de produits défectueux, *in D.*, 31e cahier, chron.
- [42] Wallerman, A. (2018), Pie in the sky when you die? Civil liability of notified bodies under the Medical Devices Directive: Schmitt. *Common Market Law Review*, 55.
- [43] Weber, R. (2017) Liability in the Internet of Things. *Journal of Consumer and Market Law*, 6(5), pp. 207-212.